MODELING HOMELAND SECURITY:
A VALUE FOCUSED THINKING APPROACH

THESIS

Kristopher Adam Pruitt, Second Lieutenant, USAF

AFIT/GOR/ENS/03-19

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GOR/ENS/03-19

MODELING HOMELAND SECURITY: A VALUE FOCUSED THINKING APPROACH

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Kristopher Adam Pruitt, BS

Second Lieutenant, USAF

March 2003

AFIT/GOR/ENS/03-19

MODELING HOMELAND SECURITY:
A VALUE FOCUSED THINKING APPROACH

Kristopher Adam Pruitt, BS
Second Lieutenant, USAF

Approved:

Richard F. Deckro, DBA (Chairman) Professor of Operations Research	date
Stephen P. Chambal, Capt, USAF (Member) Assistant Professor of Operations Research	date

Acknowledgments

The completion of this thesis effort would not have been possible without the assistance of an array of individuals. I would first like to thank my thesis advisor, Dr. Richard Deckro, whose vast knowledge of a wide variety of fields was critical in enhancing the robustness of my work. His insight and guidance were helpful in focusing the pervasive problem that my research attempted to tackle.

Secondly, I am extremely grateful for the assistance I received from my reader, Capt Stephen Chambal. His direction and contributions were above and beyond what is normally asked of a reader. In stressful times, which were many, he provided the mentorship necessary to keep me on track; always reminding me to strike a balance between education and family.

Additionally, my work would not have been nearly as successful if it were not for the help of my many classmates. They too played a big part in maintaining my composure and desire to strive for excellence. In particular, I would like to thank LCDR Johnathan Duff who went out of his way to provide me with vital points of contact. These contacts will be critical to future work in this area.

Finally, and *most* importantly, I am eternally grateful to my wife and daughter. Their patience and understanding were limitless. It would have been impossible for me to complete this program if it were not for the love and support that they have provided me over the last 18 months. In particular, my wife has been my greatest supporter and the most wonderful friend that a husband could ask for. Her support, along with that of all my family and friends was greatly appreciated.

Table of Contents

Page

Page

List of Figures

Page

List of Tables

Page

ABSTRACT

The events of September 11, 2001 have propelled the topic of homeland security to the forefront of national concern. The threat of terrorism within the United States has reached an unprecedented level. The pervasive vulnerabilities of the nation's critical infrastructure coupled with the destructive capabilities and deadly intentions of modern terrorists pose extraordinary risks. The United States must mitigate these risks while at the same time balancing the associated costs and impact on civil liberties.

Currently, the United States lacks effective methods and measures for assessing the security of the homeland from acts of terrorism. This study outlines a first cut decision analysis methodology for identifying and structuring key homeland security objectives and facilitating the measurement of the United States' capability to execute these objectives.

MODELING HOMELAND SECURITY: A VALUE-FOCUSED THINKING APPROACH

1. Introduction

1.1 Background

> America will become increasingly vulnerable to hostile attack…States, terrorists, and other disaffected groups will acquire weapons of mass destruction and mass disruption, and some will use them. Americans will likely die on American soil, possibly in large numbers. (The United States Commission, 1999:4)

This prolific statement by the Hart-Rudman Commission held true on 11 September 2001. The attacks on the World Trade Center and the Pentagon presented a definitive statement of just how real the terrorist threat to the American homeland has become. However, the threat of terrorism against the United States did not begin on 9/11. Indeed, the United States has combated terrorist acts throughout its history. Nevertheless, the face of terrorism has changed dramatically over the years (Report of the National Commission, 2000:6). The modern age of terrorist attacks against the United States, especially on the American homeland, began in the last decade of the 20th century and the threat continues to increase.

The Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02) defines terrorism as,

> The calculated use of unlawful violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the

> pursuit of goals that are generally political, religious, or ideological. (JP 1-02, 2001:437)

Furthermore, the potential threat itself (the terrorist) is defined as "an individual who uses violence, terror, and intimidation to achieve a result" (JP 1-02, 2001:437). A terrorist can be an American citizen or a foreigner, and can act alone or as part of a group.

However, not all terrorists or terrorist groups should be considered a threat to the United States. Dr. Lani Kass at the National War College utilizes the following model of the threat to the American homeland:

Vulnerabilities x Intentions x Capabilities = Threat. (Larson, 2000:5)

Increases in any one of these factors will produce increases in the threat to America. On the other hand, if any one of these factors is minimal or non-existent, then the threat is minimal or non-existent. For example, many of our allies may have the capabilities to exploit our vulnerabilities, but their lack of intent eliminates them as a threat. Unfortunately, with regards to terrorism in the United States, all three of these factors exist in some form and have been on the rise. In the face of limited resources it will be necessary to mitigate the risks associated with this amplification. An examination of America's vulnerabilities, and the intentions and capabilities of modern terrorists can provide great insight into the growing threat of terrorism.

Joint Publication 1-02 (JP 1-02) defines vulnerability as,

> The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 1-02, 2001:464)

With regards to the vulnerability of the American homeland to terrorism, this definition might be modified to be the following:

> The susceptibility of a nation to any action by any means through which the physical well-being of its people may be reduced or their way of life diminished.

America's increasing vulnerability to terrorist acts received new emphasis in the early 1990's. Following the attacks on the World Trade Center on 26 February 1993 and the A.P. Murrah Federal Building in Oklahoma City on 19 April 1995, Washington released Presidential Decision Directive 39 (PDD 39). This classified document spelled out the United States' policy on counter-terrorism (PDD 39, 1995:1). The available, unclassified version provides limited insight into how the government will respond to terrorist acts; however, it does elaborate on methods of reducing vulnerabilities (PDD 39, 1995:1). Specifically, PDD 39 mandated that the Attorney General will "chair a Cabinet Committee to review the vulnerability to terrorism of government facilities in the United States and critical national infrastructure" and report the committee's findings to the President (PDD 39, 1995:1).

In adherence to this order, Attorney General Janet Reno responded by establishing the Critical Infrastructure Working Group (CIWG) to provide an initial examination of the threat to the nations critical infrastructures (Reno, 1996:2). Guidance provided by the CIWG eventually led to the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) whose mission it was to fully assess the vulnerabilities of the nation's critical infrastructures (Reno, 1996:2, PCCIP Overview, 1997:5). The PCCIP found increasing vulnerabilities to not only physical attack but also to the new found cyber threat (Thinking Differently, 1997:3). The Commission noted the Y2K problem as a profound example of how vulnerable the nation has become as a result of its reliance on computers (Critical Foundations, 1997:11). In addition, the pervasive use of

Supervisory Control and Data Acquisition (SCADA) systems for control of infrastructure systems provides an increasing ability for terrorists to cause serious damage by cyber means (Critical Foundations, 1997:12).

Because computers and computer technology have become the basis of operations and an indispensable resource for businesses, industries, institutions, and individuals throughout the United States, a cyber-based attack could be just as effective as a physical attack. Continual increases in the use of advancing information technology (IT) have created a computer-based linkage between the nation's infrastructures. This linkage provides improvements in efficiency but presents new vulnerabilities. It is for these reasons that Presidential Decision Directive 62 (PDD 62) and Presidential Decision Directive 63 (PDD 63) were released in 1998 (PDD 62, 1998:1, PDD 63, 1998:1).

PDD 62 and PDD 63 addressed the nation's growing vulnerability to terrorist attacks and the need to protect our infrastructures. PDD 63 mandated that all critical infrastructure vulnerabilities would be assessed, and plans to reduce those vulnerabilities would be created, as part of an overarching goal to achieve full critical infrastructure protection (CIP) capability by May 2003 (PDD 63, 1998:2). Unfortunately, many of these vulnerabilities have yet to be adequately examined and no complete national infrastructure protection plan has been developed (Gross, 2001:6, National Strategy, 2002:ix). Thus, there has been a noted increase in America's vulnerability to terrorism but no completely effective effort to reduce it.

JP 1-02 defines intention as, "An aim or design (as distinct from capability) to execute a specified course of action" (JP 1-02, 2001:219). The intentions, or objectives, of today's terrorists have not necessarily increased as much as they have become more

deadly (Countering the Changing Threat, 2000:9). In fact, the number of worldwide terrorist incidents decreased dramatically throughout the 1990's, almost halving between 1991 and 1996 (Lesser, 1999:11). However, the percentage of terrorist incidents resulting in fatalities has increased (Lesser, 1999:10). In 1996, the worldwide death toll due to terrorism (510 persons) ranked as the fourth highest on record since 1968 (Lesser, 1999:12). Unfortunately, this number seems to pail in comparison with the thousands that died, on American soil alone, in 2001. The National Commission on Terrorism noted that:

> Terrorist attacks are becoming more lethal. Most terrorist organizations active in the 1970s and 1980s had clear political objectives. They tried to calibrate their attacks to produce just enough bloodshed to get attention for their cause, but not so much as to alienate public support…Now, a growing percentage of terrorist attacks are designed to kill as many people as possible. In the 1990s a terrorist incident was almost 20 percent more likely to result in death or injury than an incident two decades ago. (Report of the National Commission, 2000:6)

This trend toward higher casualties has been reflected in the increased level of security at events that were previously of limited concern. The security at numerous sporting events (the 2002 Winter Olympics and the Super Bowl, for example) and at a variety of large public gatherings (such as New Years and July 4th celebrations) presents a clear example of this newfound concern over the American public as a target. The bombings of the World Trade Center in both 1993 and 2001, the Khobar Towers in Saudi Arabia, and the U.S. embassies in Africa display more of a desire to inflict casualties than to achieve political objectives (Report of the National Commission, 2000:6). The motivation for modern terrorists such as Osama Bin Laden and his al-Queda network is largely couched in religious and based on hatred for the United States government, as

well as a desire to display the reach of their abilities in order to recruit like minded people (Report of the National Commission, 2000:6). The radically different value systems and methods of legitimization and justification that these religious terrorist groups harbor make them potentially far more dangerous than more traditional, secular terrorists like the Irish Republican Army (Lesser, 1999:19-20, Report of the National Commission, 2000:6). For religious terrorists, violence and death are "divine duties" to be carried out against anyone who does not share their beliefs (Lesser, 1999:20). Thus, the level of deadly intent has significantly increased with today's terrorists.

Finally, the capabilities of today's terrorist far outweigh those of the past. JP 1-02 defines capability as, "The ability to execute a specified course of action (A capability may or may not be accompanied by an intention)" (JP 1-02, 2001:62). The proliferation of chemical, biological, radiological, and nuclear weapons, coupled with increased access to the technologies necessary to use these weapons, has created new opportunities for terrorists intent on inflicting harm (Proliferation, 2001:61). The issue of proliferation is complicated further by the fact that states such as Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria have been identified as sponsors and supporters of terrorism (Lesser, 1999:14).

Though the likelihood of states providing terrorist groups with weapons of mass destruction (WMD) is believed to be low, the capability of many groups to acquire the technology on their own is increasing (Proliferation, 2001:61). The sarin nerve gas attacks on the Tokyo subway in 1995 and the Anthrax scares in America in 2001 are just two examples of the worldwide capability of terrorist networks to use WMD. In addition, funding from dissident millionaires like Osama Bin Laden reduces the need to be fully

supported by a sponsoring state. Bin Laden has repeatedly expressed his interest in obtaining WMD for use against the United States and likens it to a religious duty (Proliferation, 2001:62). However, WMD are not the only increasingly accessible capabilities that the United States needs to be concerned with.

The Information Age has brought about a new potential for anyone with a computer to use it as a weapon. The number of computer literate individuals worldwide has increased exponentially as the cost of obtaining a computer has dropped. This advancement has offered new opportunities for global communication and commerce but has also enhanced the capability of individuals with less reputable intent. Indeed, viruses and other computer-based means of attack are easily attainable for anyone connected to the Internet. These range from sophisticated tools requiring expert knowledge to effectively utilize them to so called "script kiddie" tools that require little to no skills to carry out an attack. Because of this interconnectedness, today's criminals, as well as terrorists, have a worldwide reach. Given the critical infrastructure vulnerabilities mentioned previously, this new capability is of great concern.

The terrorist threat to the United States is dramatically increasing. The vulnerabilities of our infrastructures, and thus our nation, are directly correlated to our growing dependence on computer power. The deadly intent of religiously motivated terrorists has increased along with their hatred for our government and way of life. Finally, the capability of today's terrorist to acquire and deliver both traditional and cyber weapons is on the rise.

Since 11 September 2001 the United States government's response to the threat of terrorism has been profound. Less than one month after the attacks on 9/11 President

Bush released Executive Order 13228, establishing the Office of Homeland Security and the Homeland Security Council (EO 13228, 2001:1). The President's intention was for the Office to develop and coordinate implementation of a national strategy for "detecting, preparing for, preventing, protecting against, responding to, and recovering from terrorist threats or attacks within the United States" (EO 13228, 2001:1). Even before the plan was completed and released, in July 2002, it became apparent that the challenges brought on by protecting the homeland would require bold Federal government reorganization. With this in mind, in June 2002 the President called for the creation of the Department of Homeland Security (Bush, 2002:1). Legislation to implement the President's plan received Congressional approval in November 2002 and the Department was established. As the "most significant transformation of the U.S. government in over a half-century," this endeavor will combine a plethora of government organizations into a single department whose overriding mission is to protect our homeland from terrorism (Bush, 2002:1).

The objectives for homeland security delineated in the National Strategy, of which the Department of Homeland Security is a part, are the following:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur. (National Strategy, 2002:2)

The nation as a whole must make every effort to execute these objectives in order to secure the United States homeland from terrorist threats and attacks. On the other hand, it would be virtually impossible to prevent *every* form of terrorist attack, reduce the vulnerabilities of *every* asset, or prepare to respond to *every* conceivable threat without

unacceptable infringements on the rights of the nation's citizenry and astronomic resource costs. Accordingly, it is vital that decision-maker's at the highest levels of authority assist in weighting these considerations against one another in the development and implementation of homeland security strategy.

1.2 Problem Statement

> Because the number of potential terrorist acts is nearly infinite, we must make difficult choices about how to allocate resources against those risks that pose the greatest danger to our homeland. (National Strategy, 2002:3)

Ensuring the security of the American homeland from terrorism is one of the most fundamental duties of the United States government. Unfortunately, only a finite number of resources exist to accomplish this mission. Thus, it becomes necessary to examine the delicate balance between the competing objectives of securing the nation from terrorism, maintaining the individual liberties of its citizens and avoiding excessive resource costs (National Strategy, 2002:2). An accurate assessment of these objectives requires a thorough identification and clarification of what is important in the decision process involved with developing methods for securing the homeland. In addition, such an assessment must consider the potential negative impacts that security efforts incur. This thesis provides a decision support framework for Federal level homeland security decision-makers to leverage in the development and evaluation of alternative homeland security strategies, taking into account both positive and negative impacts.

1.3 Problem Approach

Because the terrorist threat to our nation is continually evolving, the methods of security must also evolve. Therefore, a study focused solely on each and every conceivable threat would be infinite. However, analysis focused specifically on what is valued (i.e. what is important) in security solutions will provide a more long-term method for evaluating the consequences of homeland security decisions. Keeney developed a value-based decision-making process to address issues such as this.

Keeney's Value Focused Thinking (VFT) approach allows for the analysis of trade-offs between what is valued. With regards to homeland security, potential value trade-offs exist between the level of security, impact on civil liberties, and resource allocation. Keeney describes this conflict of values as a situation where the nation can "enhance the manifestation of one value only if [it accepts] a degradation in the manifestation of another value" (Keeney, 2001:1). To accurately judge value trade-offs, the following is required:

- A clear understanding of all of the fundamental objectives influenced by competing alternatives being considered;
- A recognition of the value trade-offs that exist; and
- A willingness to think hard about and make necessary value trade-offs. (Keeney, 2001:1)

This thesis develops the first two requirements in order to assist the Federal government in accomplishing the third requirement. The choice of VFT as the methodology to accomplish these tasks is largely based on its successful application in the energy industry, manufacturing and services community, and the military. In Chapter 2 of this

thesis, the successful application of VFT in two national level studies, *SPACECAST 2020* and *AIR FORCE 2025*, is discussed in more detail.

The identification of the appropriate objectives and associated values was accomplished through a comprehensive examination of the homeland security literature and other relevant doctrine, to include the United States Constitution.

1.4 Research Scope

This thesis addresses the development of homeland security strategy at the *federal* level. A national perspective is a shared responsibility that inherently includes federal, state, and local governments, as well as the private sector and the American people (National Strategy, 2002:2). However, because the Federal government has the primary responsibility for organizing the security of the nation, a method for developing and ranking alternatives at this level is vital. This decision structure can then be utilized in subsequent research to create similar support tools for lower levels of government and the private sector.

This study is a first cut effort to apply the VFT methodology to the homeland security decision context. Because of the complexity of the problem and the resources available to complete this thesis, only the initial stages of the VFT analysis are addressed. However, as a first step in the more complete analysis of this issue, it is vital that the initial stages are completely and accurately addressed. Further studies, with the support of homeland security decision-makers and subject matter experts, will then have the proper foundation to address the remaining stages of the analysis.

1.5 Thesis Outline

Following this introduction, Chapter 2 of this thesis provides a review of the pertinent literature in the realm of homeland security. Included in Chapter 2 is a brief review of the VFT methodology and some of its applications. As an embellishment to that review, Chapter 3 articulates more thoroughly the specific methodology employed in this research including the problem definition, the development of the value hierarchy, the creation of evaluation measures, and the construction of single dimension value functions. Chapter 4 then applies that methodology to the homeland security decision context and provides the subsequent results. Finally, Chapter 5 delineates the conclusions and recommendations drawn from the aforementioned analysis.

2. Literature Review

Since the attacks on 11 September 2001 homeland security has been widely recognized as a paramount concern to the United States. As a result, there exists a plethora of documents pertaining to what homeland security is and is not, how it should be carried out, and who should be responsible for doing so. The purpose of this review is to identify the resources (articles, reports, doctrine, and so forth) necessary to develop a clear understanding of what is valued at the national executive level in homeland security and to provide sufficient support for the application of value-focused thinking to the homeland security problem.

2.1 Prior to September 11th

The security of the American homeland has been given some level of priority since the colonial days. The concern for homeland security, prior to 9/11, peaked in the 1950's when the Cold War prompted an emphasis on civil defense (Larsen, 2002:np). However, the focus on protecting the United States from asymmetrical threats, such as terrorism, only became prominent in the late 1990's (McIntyre, 2002:np).

2.1.1 The National Defense Panel

The National Defense Panel released its report, entitled "Transforming Defense: National Security in the 21st Century," in 1997. Philip A. Odeen, the chairman of the panel, wrote:

> Our report focuses on the long-term issues facing U.S. defense and national security. It identifies the changes that will be needed to ensure U.S. leadership and the security and prosperity of the American people in the twenty-first century. We are convinced that the challenges of the twenty-first century will be quantitatively and qualitatively different from those of the Cold War and require fundamental change to our national security institutions, military strategy, and defense posture by 2020. (National Defense Panel, 1997:np)

It was in this report that the term *homeland defense* (a subset of homeland security) first received notoriety (National Defense Panel, 1997:25, McIntyre, 2002a:np). Homeland defense only addresses the efforts to deter or defend against attacks, while homeland security encompasses these efforts as well as the response to attacks and other responsibilities (McIntyre, 2002a:np). The changing threat to the United States prompted the need for new thinking about how to protect America and its citizenry. In addition to the continued need to deter state sponsored nuclear attacks, the Panel recognized the newfound necessity to "defend against terrorism, information warfare, weapons of mass destruction, ballistic and cruise missiles, and other transnational threats to the sovereign territory of the nation" (National Defense Panel, 1997:25). To combat the challenges brought on by the changing threat to America, the Panel recommended the following initiatives:

- Develop integrated active and passive defense measures against the use of WMD.
- Develop and retain the option to deploy a missile defense system capable of defeating limited attacks.
- Incorporate all levels of government into managing the consequences of a WMD-type attack.
- Prepare reserve components to support consequence management activities.
- Support the recommendations of the President's Commission on Critical Infrastructure Protection.
- Use Department of Defense assets to advise and assist law enforcement in combating terrorist activities. (National Defense Panel, 1997:28)

Though these recommendations were only targeted toward a portion of homeland security, that is homeland defense, they emphasized the need for new thinking in the security of America. Following the National Defense Panel's report, several other commissions and panels presented research and recommendations further stressing the importance of homeland security.

2.1.2 Homeland Security Commissions

The Hart-Rudman Commission

On 15 September 1999 The United States Commission on National Security/21st Century released the first of what would be three reports on the emerging global security environment for the first quarter of the 21st century. The commission was co-chaired by former Senators Gary Hart and Warren B. Rudman. This first report, titled *New World Coming: American Security in the 21st Century*, delineated an array of assumptions about the future on which the commission would base their study. These assumptions covered an array of topics, including the political, economic, military, and cultural position of the United States in the next quarter century (The United States Commission, 1999:3). Based on these assumptions, the commission developed a list of conclusions regarding the future security of the United States. Most prominent among these conclusions was the statement that the American homeland will become increasingly more vulnerable to hostile attack (The United States Commission, 1999:4). Advances in information technology will create new vulnerabilities in economic and other infrastructures (The United States Commission, 1999:4). Overall, the commission concluded that "for many

years to come Americans will become increasingly less secure, and much less secure than they now believe themselves to be" (The United States Commission, 1999:8). Driven by this fact, the commission sought to develop a national strategy for the security of the homeland in its Phase II report (The United States Commission, 1999:8).

The Phase II report, *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom*, was released seven months later. In this study the commission suggested the "strategic precepts that should guide the formulation of U.S. strategy, and then [took] a fresh look at U.S. national interests and priority objectives" (The United States Commission, 2000:5). On that basis, the commission developed a framework for a new national security strategy (The United States Commission, 2000:5). In developing strategy, certain issues must be taken into consideration.

> Freedom is the quintessential American value, but without security, and the relative stability that results there-from, it can be evanescent. American strategy should seek both security and freedom, and it must seek them increasingly in concert with others. (The United States Commission, 2000:6)

Additionally, any national security strategy should be grounded in U.S. interests at three levels; survival, critical, and significant (The United States Commission, 2000:7). Survival interests are those without which America would cease to exist as it currently does (The United States Commission, 2000:7). Such interests include defense from direct attack and the preservation of Constitutional order (The United States Commission, 2000:7). Critical national interests include the continuity and security of the key infrastructures on which Americans are dependant (The United States Commission, 2000:7). Finally, the United States has a significant interest in the spread abroad of "constitutional democracy under the rule of law, market-based economics, and universal

recognition of basic human rights" (The United States Commission, 2000:7). Based on these interests, the U.S. must prioritize and execute a variety of security related objectives.

The Hart-Rudman Commission listed the following six objectives as key to the future security of the nation.

- Defend the United States and ensure that it is safe from the dangers of a new era.
- Maintain America's social cohesion, economic competitiveness, technological ingenuity, and military strength.
- Assist the integration of key major powers, especially China, Russia, and India, into the mainstream of the emerging national system.
- Promote, with others, the dynamism of the new global economy and improve the effectiveness of international institutions and international law.
- Adapt U.S. alliances and other regional mechanisms to a new era in which America's partners seek greater autonomy and responsibility.
- Help the international community tame the disintegrative forces spawned by an era of change. (The United States Commission, 2000:8-13)

As part of executing these objectives, the Commission stressed that the United States must enhance the military and civil aspects of homeland security (The United States Commission, 2000:14-15). In particular, the commission recognized the need to train and equip the National Guard to assume a significant role in defending the homeland (The United States Commission, 2000:15).

In addition to outlining the objectives and priorities necessary to develop a national security strategy, the commission pointed out that the U.S. government is not properly organized in a manner conducive to executing such a strategy (The United States Commission, 2000:16). Thus, the third and final report addressed the need to restructure the U.S. government to address the rising threat.

Road Map for National Security: Imperative for Change was released on 31 January 2001. The commission stated,

> After our examination of the new strategic environment of the next quarter century (Phase I) and of the strategy to address it (Phase II), this Commission concludes that significant changes must be made in the structures and processes of the U.S. national security apparatus. Our institutional base is in decline and must be rebuilt. Otherwise the United States risks losing its global influence and critical leadership role. (The United States Commission, 2001:viii)

Recommendations for organizational change were made in five key areas.

- Ensuring the security of the American homeland;
- Recapitalizing America's strengths in science and education;
- Redesigning key institutions of the Executive Branch;
- Overhauling the U.S. government personnel system;
- Reorganizing Congress's role in national security affairs. (The United States Commission, 2001:viii)

It is the first recommendation that is of particular interest to this research.

The commission noted the end of the United States' veritable invulnerability to direct attack due to the enhanced proliferation of unconventional weapons and the persistence of international terrorists (The United States Commission, 2001:viii). In addition, the commission stated that "a direct attack against American citizens *on American soil* is likely over the next quarter century" (The United States Commission, 2001:viii). Given the growing risk, it was recommended that a National Homeland Security Agency (NHSA) be created to assume responsibility for planning, coordinating, and integrating an array of U.S. government homeland security activities (The United States Commission, 2001:viii). This Cabinet level organization would integrate the Federal Emergency Management Agency, Coast Guard, Customs Service, the Border Patrol, and various agencies with responsibility for critical infrastructure protection (The

United States Commission, 2001:viii). This recommendation was a prelude to the Department of Homeland Security currently being stood up.

Additionally, the commission acknowledged the need to further develop the participation of the Department of Defense (DOD) in this mission area (The United States Commission, 2001:ix). Accordingly, it recommended the creation of the office of the Assistant Secretary for Homeland Security to oversee DOD homeland security activities and to ensure that the necessary resources are made available (The United States Commission, 2001:ix). Along with increased DOD participation, and as stated in its Phase II report, the commission suggested that the National Guard be given homeland security as its primary mission (The United States Commission, 2001:ix).

Finally, with regards to ensuring the security of the American homeland, the commission recommended the reorganization of Congress to accommodate the Executive Branch realignment and to provide general support for the homeland security mission area (The United States Commission, 2001:ix).

The Gilmore Commission

On 15 December 1999 the Advisory Panel to Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction released their first annual report to the President and Congress. Led by Governor James S. Gilmore III, the commission is often referred to as the Gilmore Commission. In its report the commission noted the new challenges presented by modern terrorists.

> As we stand on the threshold of the twenty-first century, the stark reality is that the face and character of terrorism are changing and that previous

> beliefs about the restraint on terrorist use of chemical, biological, radiological, and nuclear (CBRN) devices may be disappearing. Beyond the potential loss of life and the infliction of wanton casualties, and the structural or environmental damage that might result from such an attack, our civil liberties, our economy, and indeed our democratic ideals could also be threatened. The challenge for the United States is first to deter and, failing that, to be able to detect and interdict terrorists before they strike. Should an attack occur, we must be confident that local, state, and Federal authorities are well prepared to respond and to address the consequences of the entire spectrum of violent acts. (Advisory Panel, 1999:vi)

Thus, it is vital that the United States not only provides security from terrorism, but also recognizes the importance of civil liberties and the economy. Given the new thinking necessary to address the threat of terrorism, the Panel was tasked with assessing the Federal governments current efforts to enhance preparedness in order to identify deficiencies (Advisory Panel, 1999:vii). Further, the commission was directed to recommend effective response options and funding at the federal, state, and local level (Advisory Panel, 1999:vii).

The Panel concluded that the United States needs a viable national strategy that clearly delineates federal, state, and local roles and responsibilities, recognizing that the Federal government must be supportive of state and local authorities who traditionally have the responsibility to respond (Advisory Panel, 1999:ix-x). In addition, it is vital that comprehensive threat and vulnerability assessments continue to be performed to support the decision-making of policymakers (Advisory Panel, 1999:x). The Panel further concluded that the complexity of the anti-terrorism effort suggests that terms and issues should be more universally defined and that this information needs to be more effectively distributed to all levels of government (Advisory Panel, 1999:x). Finally, the commission noted that national standardization of planning, training, and equipping

among responders and their command and control entities is critical (Advisory Panel, 1999:xi).

Exactly one year after their first report, the Advisory Panel released the second installment, *Toward a National Strategy for Combating Terrorism*. The Panel continued to recognize the growing threat of terrorist attacks within the United States.

> The terrorist incidents in this country—however tragic—have occurred so rarely that the foundations of our society or our form of government have not been threatened. Nevertheless, the potential for terrorist attacks inside the borders of the United States is a serious emerging threat. There is no guarantee that our comparatively secure domestic sanctuary will always remain so. Because the stakes are so high, our nation's leaders must take seriously the possibility of an escalation of terrorist violence against the homeland. (Advisory Panel, 2000:ii)

However, in its second year the Advisory Panel shifted its focus from threat assessment to specific programs to combat terrorism and larger questions of national strategy (Advisory Panel, 2000:ii). In particular, the commission emphasized problems in the Federal Executive Branch (Advisory Panel, 2000:ii-iii). Their recommendation was that, given no coherent, functional national strategy for combating terrorism existed, the incoming President should develop and release such a strategy within one year of assuming office (Advisory Panel, 2000:iii). The Panel pointed out that a truly comprehensive national strategy would include not only federal responsibilities, but state and local roles as well (Advisory Panel, 2000:iv). In addition, the strategy should be based on measurable performance objectives that meet the overall objectives of deterrence, prevention, preparedness, and response (Advisory Panel, 2000:iv).

Along with a national strategy, the Advisory Panel found that uncoordinated and fragmented efforts by the Federal government to combat terrorism required a centralized

office and committee within the Executive Branch and Congress respectively (Advisory Panel, 2000:v-vii). These organizations could then assist the Federal government in supporting State and local capabilities to combat terrorism (Advisory Panel, 2000:viii).

Overall, the Panel noted numerous deficiencies in the Federal government's preparedness to secure the United States from terrorist attacks. Its recommendations to develop a national strategy and create organizations specifically designed to combat terrorism provided insight to actions the United States could take to address the risk to the homeland. Unfortunately, the advise of the Panel was not fully heeded until *after* the tragic events of 9/11.

The Bremer Commission

On 7 June 2000 the National Commission on Terrorism presented its report, *Countering the Changing Threat of International Terrorism*, to Congress. Chaired by Ambassador L. Paul Bremer III, the commission was mandated with evaluating America's laws, policies, and practices for preventing and punishing terrorism directed at American citizens (National Commission, 2000:2). In the development of its report, four important points were continually under consideration.

- The imperative to find terrorists and prevent their attacks requires energetic use of all the legal authorities and instruments available.
- Terrorist attacks against America threaten more than the tragic loss of individual lives. Some terrorists hope to provoke a response that undermines our Constitutional system of government. So U.S. leaders must find the appropriate balance by adopting counterterrorism policies which are effective but also respect the democratic traditions which are the bedrock of America's strength.
- Combating terrorism should not be used as a pretext for discrimination against any segment of society. Terrorists often claim to act on behalf of ethnic

groups, religions, or even entire nations. These claims are false. Terrorists represent only a minuscule faction of any such group.

- People turn to terrorism for various reasons. Many terrorists act from political, ideological, or religious convictions. Some are simply criminals for hire. Others become terrorists because of perceived oppression or economic deprivation. An astute American foreign policy must take into account the reasons people turn to terror and, where appropriate and feasible, address them. No cause, however, justifies terrorism. (National Commission, 2000:2)

Keeping these ideas in mind, the commission addressed the growing threat of terrorism within the United States. It noted that all efforts must be made to collect intelligence about terrorist plans and that this information must be applied to disrupting and prosecuting terrorist activities and sources of support (National Commission, 2000:3). This includes government support and funding for increased authority and capabilities for the FBI, CIA, and NSA in order to obtain the needed information (National Commission, 2000:3). They note that the United States should use every available means to target both the State and private sources of financial and logistical support terrorists need to carry out their attacks (National Commission, 2000:3).

Furthermore, federal, state, and local officials must be prepared to respond to attacks that do occur (National Commission, 2000:3). Due to the destructive potential of chemical, biological, radiological, nuclear, and cyber weapons the commission recommended that extensive planning and exercises be carried out to ensure the capabilities and coordination of response entities (National Commission, 2000:4). Additionally, the United States should work along with other countries worldwide to prevent unauthorized access to weapons of mass destruction (National Commission, 2000:4).

The recommendations of the Bremer Commission were in general agreement with the finding of the Gilmore Commission. The increased threat of vastly destructive terrorist attacks within the United States required significant government action to prevent such attacks and to prepare for the possibility that prevention fails. Addressing this threat will require new thinking about laws, policies, and practices, and increased planning, training, and exercises.

Overall, the insight and recommendations offered by all three of these homeland security commissions (Hart-Rudman, Gilmore, and Bremer) appear to have significantly influenced homeland security policies and action. The predictions of increasing threats to the American homeland were sadly proven true by the devastating attacks on 9/11. The suggested development of a comprehensive strategy to secure the United States was realized in July 2002 when the *National Strategy for Homeland Security* was released by the Office of Homeland Security. This new Office, along with the Department of Homeland Security, has addressed the recommended reorganization of the Federal government to combat the terrorist threat to America.

2.2 Critical Infrastructure Protection

> **Infrastructure**: The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole. (Critical Foundations, 1997:B-2)
>
> **Critical Infrastructure**: Infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security. (Critical Foundations, 1997:B-1)

Technological advances in the dissemination of information, while creating an array of improvements, have posed new problems for the security of the nation. Computers and computer technology have become the basis of modern operations and an indispensable resource for businesses, industries, institutions, and individuals throughout the United States.

The infrastructures of the nation are no exception. In his proposal for the Department of Homeland Security, President Bush recognized that infrastructure sectors such as "food, water, agriculture, health systems and emergency services, energy, transportation, information and telecommunications, banking and finance, defense industry, postal and shipping, and national monuments and icons" all rely heavily on computer power (Bush, 2002:15). Advances in information technology (IT) have increased the efficiency of these infrastructures; however, those same advances have amplified their interdependence (PDD 63, 1998:1). As a result of this newfound interdependence, the nation's infrastructures are increasingly vulnerable to both physical and cyber attacks. The results of an attack, whether physical or electronic, on the infrastructures' cyber-based linkage could cascade across many sectors inflicting damage on the nation's essential services and economy (Bush, 2002:15).

Thus, it becomes increasingly important to identify infrastructure vulnerabilities and develop defense strategies that include prioritization of critical infrastructure protection (CIP) initiatives. Because it is not feasible to completely protect every critical infrastructure, methods of prioritization are paramount. Presidential Decision Directive 63 (PDD 63), the Clinton Administration's Policy on CIP, provides a framework for developing critical infrastructure defense strategies. The goals laid out in PDD 63

address the CIP problem in detail, clearly defining the nation's civilian critical infrastructures and mandating a variety of actions for all levels of government.

Elaborating on the definition given by the PCCIP, PDD 63 defined critical infrastructures to be "those physical and cyber-based systems essential to the minimum operations of the economy and government" (PDD 63, 1998:1). The time constraints mandated in PDD 63 imply that by the year 2000 there should be an initial capability to protect the United States' critical infrastructures and that full CIP ability will be achieved by May 22, 2003 (PDD 63, 1998:2). Full protection capability is defined as the ability to protect the nation from "intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services." (PDD 63, 1998:2)

The document further directed that any interruptions in these functions must be sporadic and inconsequential to the welfare of the United States (PDD 63, 1998:2). Thus, PDD 63 provided focus to the complex problem of protecting the nation's critical infrastructures. However, defining the problem and formulating a solution are two very distinct issues.

The directive continued by specifying necessary steps to reduce the vulnerability of the above functions. PDD 63 specified that Lead Agencies in charge of protecting specific infrastructures would appoint Sector Liaison Officials to work closely with private sector officials in the same sectors of interest (PDD 63, 1998:2). This team of sector officials was tasked with developing a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack. (PDD 63, 1998:2-3)

The aforementioned plan was thus intended to identify areas that need to be hardened, develop plans to harden them, create systems to assess when these hardened targets are being attacked, and to then develop a warning and response plan.

In addition, PDD 63 found that particular attention should be paid to developing a system to continually assess the reliability, vulnerability, and threat level of our critical infrastructures (PDD 63, 1998:3). The purpose of this requirement was to provide a continuous status report that can be used for strategy and response planning.

The Bush administration has since renewed this effort with the release of the USA Patriot Act. Section 1016, titled the Critical Infrastructure Protection Act of 2001, details the need for extensive modeling and analysis in order to ensure the stability of the interdependent network of critical infrastructures and to provide a basis for CIP policy recommendations (107th, 2001:338). The act created the National Infrastructure Simulation and Analysis Center (NISAC) to take the lead in this field (107th, 2001:339). The NISAC is to provide the guidance necessary to develop a more thorough understanding of the large-scale complexity of our critical infrastructures and how to modify them in order to mitigate threats (107th, 2001:340).

However, the primary missions involving the protection of our critical infrastructures are the responsibility of the Lead Agencies assigned to each sector. For each vital national infrastructure, U.S. Government departments and organizations were

assigned as the lead agencies for liaison with the private sector (PDD 63, 1998:4). It is the responsibility of these agencies to work with the appropriate private sector officials to develop the portion of the National Infrastructure Assurance Plan pertinent to their sector (PDD 63, 1998:4). These Lead Agencies were assigned as follows:

- Information and communication → Department of Commerce
- Banking and Finance → Department of the Treasury
- Water Supply → Environmental Protection Agency
- Transportation → Department of Transportation
- Emergency services → Department of Justice (DOJ)
  Federal Bureau of Investigation (FBI)
  Federal Emergency Management Agency (FEMA)
- Continuity of government → FEMA
- Public Health → Health and Human Services
- Electric power, oil, gas → Department of Energy.

(PDD 63, 1998:8)

In addition to protecting the individual infrastructure sectors, there exist certain duties that must be solely carried out by the Federal Government. These duties include national defense, foreign affairs, intelligence, and law enforcement (PDD 63, 1998:4). To accomplish these solely Federal tasks, Lead Agencies were assigned, however, they would not collaborate with the private sector (PDD 63, 1998:4). The Lead Agencies for Special Functions were assigned as follows:

- Law Enforcement/Internal Security → DOJ / FBI
- Foreign Intelligence → Central Intelligence Agency
- Foreign Affairs → Department of State
- National Defense → Department of Defense.

(PDD 63, 1998:8)

Given the establishment of the Department of Homeland Security, the organizations responsible for these sectors and for meeting the May 22, 2003 suspense for full critical infrastructure protection may change.

Collectively, the findings of a variety of review agencies seriously question the ability of the Federal Government to achieve the full operating capability goal by the given suspense (PCIE/ECIE, 2001:3). A lack of clarity in critical infrastructure identification and vulnerability assessment, in particular, has contributed to this problem. In addition, the General Accounting Office (GAO) has recognized that problems in developing critical infrastructure national strategy have stemmed from the unclear definition of CIP objectives and performance measures (GAO-02-961T, 2002:2). The Bush Administration has continued the efforts to remedy these problems with the establishment of the Office of Homeland Security and the Department of Homeland Security. Both organizations recognize the need to identify and prioritize objectives for defending the nation's critical infrastructures (EO 13228, 2001:2-3, National Strategy, 2002:15). Unfortunately, it appears that thus far efforts in that arena have been limited; the infrastructures so vital to the continued prosperity of the nation remain vulnerable. In particular, these vulnerabilities contribute significantly to the threat of terrorism within the United States.

2.3 The Office of Homeland Security

Less than one month after the attacks of September 11th President Bush released Executive Order 13228, establishing the Office of Homeland Security (OHS) and the

Homeland Security Council. Each of these organizations have played a key role in securing the homeland from acts of terrorism. To lead the OHS, former Governor of Pennsylvania Tom Ridge was sworn in as the Assistant to the President for Homeland Security. Governor Ridge is responsible for ensuring the accomplishment of the vital homeland security tasks delineated in Executive Order 13228.

The mission set forth for the OHS is to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks" (EO 13228, 2001:1). In carrying out its mission, the Office is tasked with coordinating the national effort to "detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States" (EO 13228, 2001:1). The OHS has made a great deal of progress in performing its mission, as the *National Strategy for Homeland Security* was successfully completed and released in July 2002. The *Strategy* is discussed in more detail in Section 2.5. of this chapter. The current section examines the functions assigned the OHS upon its establishment. Many of these responsibilities may very well change as the Department of Homeland Security is brought on line. Regardless, the OHS will "continue to play a key role, advising the President and coordinating a vastly simplified interagency process" (Bush, 2002:3).

2.3.1 Detection

The OHS is responsible for identifying priorities and coordinating efforts for collecting and analyzing information regarding the threats and activities of terrorists or terrorist groups within the United States (EO 13228, 2001:1). While the OHS is held

accountable for *facilitating* the collection of information from state and local governments within the United States, the Office is only responsible for *prioritizing* the needs for foreign intelligence related to terrorism (EO 13228, 2001:1). This prioritization can then be used as a guide by other organizations responsible for collecting foreign intelligence (EO 13228, 2001:1). Furthermore, the Office is required to coordinate efforts to ensure that executive departments and agencies have sufficient technological capabilities and resources for not only data collection, but also detection of the release of weapons of mass destruction (EO 13228, 2001:1). Finally, the OHS is tasked with ensuring that proper homeland security related intelligence is distributed to the appropriate entities (EO 13228, 2001:2).

2.3.2 Preparedness

The Office is held accountable for coordinating national efforts to "prepare for and mitigate the consequences of terrorist threats or attacks within the United States" (EO 13228, 2001:2). In order to enhance the nation's preparedness, the OHS is responsible for assessing how well Federal emergency response plans address terrorist threats or attacks (EO 13228, 2001:2). This includes the review of public health policies, pharmaceutical stockpiles, and hospital capacities (EO 13228, 2001:2). The Office must coordinate exercises and simulations to test the readiness of vital systems and to ensure the preparedness of Federal response teams (EO 13228, 2001:2). Finally, the OHS is responsible for coordinating Federal assistance to State and local authorities and

nongovernmental organizations as these entities conduct preparation activities (EO 13228, 2001:2).

2.3.3 Prevention

The OHS is tasked with coordinating efforts to prevent terrorist attacks within the United States (EO 13228, 2001:2). In doing so, the Office will work with immigration and cargo shipment authorities to obstruct the entry of terrorists and terrorist materials into the United States, as well as to facilitate removal of such terrorists when necessary (EO 13228, 2001:2). To further prevent the entry of terrorists, the OHS is responsible for coordinating efforts to enhance the security of the nation's borders, territorial waters, and airspace (EO 13228, 2001:2). Underpinning all of these prevention activities is the task of investigating terrorist threats and attacks within the United States (EO 13228, 2001:2).

2.3.4 Protection

The OHS is responsible for coordinating "efforts to protect the United States and its critical infrastructure from the consequences of terrorist attack" (EO 13228, 2001:2). This includes strengthening measures for protecting energy services, telecommunications, nuclear facilities, transportation systems, agriculture, systems for distributing food and water and other critical infrastructure services (EO 13228, 2001:3). The Office is also accountable for coordinating efforts to protect public and privately owned information systems, developing criteria for assessing the security of major public and privately owned facilities, and overseeing efforts to protect special events that are determined to be

of national significance (EO 13228, 2001:3). Finally, the Office is tasked with protecting the United States by eliminating unauthorized access to and development of weapons of mass destruction that could be used in a terrorist attack (EO 13228, 2001:3).

2.3.5 Response and Recovery

The Office is responsible for coordinating "efforts to respond to and promote recovery from terrorist threats or attacks within the United States" (EO 13228, 2001:3). As part of this responsibility, the OHS must direct efforts to ensure the rapid restoration of transportation systems, energy services, telecommunications, and other critical infrastructure facilities, as well as public and private critical information systems, in the event of a terrorist attack (EO 13228, 2001:3). The OHS is also tasked with working with the National Economic Council to coordinate efforts to stabilize national financial markets following a terrorist incident (EO 13228, 2001:3). Similarly, the Office must coordinate financial assistance, as well as medical treatment, for the victims of such incidents (EO 13228, 2001:3). Finally, in the effort to respond and recover from terrorist attacks, the OHS is responsible for coordinating the containment and removal of hazardous materials used in the attack (EO 13228, 2001:3).

2.4 The Department of Homeland Security

Prior to the release of the *National Strategy for Homeland Security* President Bush proposed a vast restructuring of the federal government to enhance the security of the nation. As the largest government transformation since the Department of Defense

was established by the National Security Act of 1947, the Department of Homeland Security combines the responsibilities of numerous government organizations into a single agency with homeland security as its primary mission (Bush, 2002:2,7). Through this consolidation, the United States has one department to coordinate efforts to secure the nation's borders and critical infrastructure, synthesize and analyze homeland security intelligence, coordinate communications with state and local governments, as well as the private sector, and protect the American people from weapons of mass destruction (Bush, 2002:2).

On 19 November 2002 the Senate approved legislation, previously approved by the House, to create the new Department (Kingsley, 2002:1). President Bush stated, "This landmark legislation, the most extensive reorganization of the federal government since the 1940's, will help our nation meet the emerging threats of terrorism in the 21st century" (Kingsley, 2002:1). The stated mission of the new Department is to:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur. (Bush, 2002:8)

In order to accomplish its mission, the Department consists of five major divisions, or "directorates" (DHS Organization, 2003:np). These five divisions are:

- Border and Transportation Security;
- Emergency Preparedness and Response;
- Science and Technology;
- Information Analysis and Infrastructure Protection; and
- Management (DHS Organization, 2003:np)

Figure 2-1 displays a more detailed breakdown of this organizational structure (DHS Organization, 2003:np).

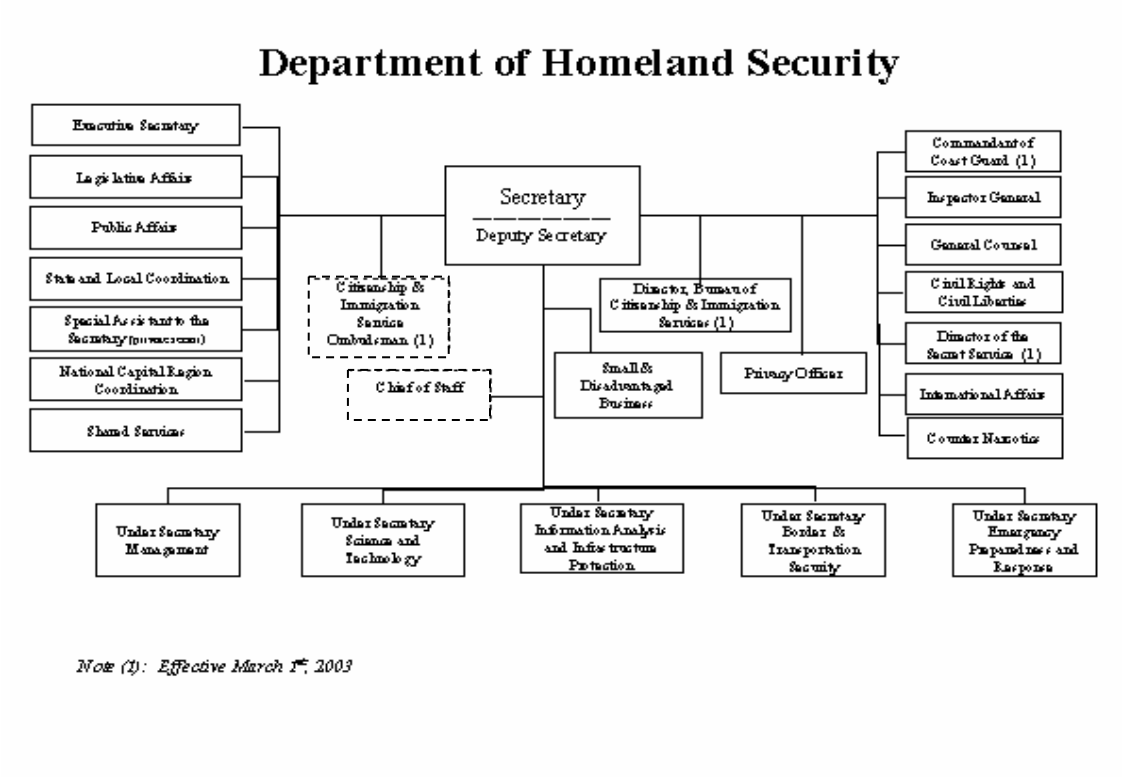

Figure 2-1: Organization of the Department of Homeland Security

Each of the mission areas associated with the five major departmental divisions is discussed below in more detail.

2.4.1 Border and Transportation Security

Securing the nation's borders includes efforts in the land, sea, air and space arenas. The logistical issues associated with such efforts are astounding.

> The United States has 5,525 miles of border with Canada and 1,989 miles with Mexico. Our maritime border includes 95,000 miles of shoreline, and a 3.4 million square mile exclusive economic zone. Each year, more than 500 million people cross the borders into the United States, some 330 million of whom are non-citizens. (Bush, 2002:9).

The Department will be responsible for who and what crosses these borders and for coordinating efforts to prevent the entry of terrorists and terrorist weapons (Bush, 2002:9). At the same time, it is vital that these security measures do not unnecessarily impede the flow of legitimate traffic into the United States (Bush, 2002:9). By enhancing border technology, intelligence, national coordination, and international cooperation the nation's borders can be made more secure while also improving day-to-day business (Bush, 2002:9). The Department will incorporate a variety of existing government organizations, including the United States Coast Guard and the Immigration and Naturalization Service (INS), to carry out its border security mission (Bush, 2002:10).

The inclusion of the Transportation Security Administration (TSA) into the Department reflects the importance of not only securing the nation's borders, but also protecting the nation's transportation systems. The tools used by the TSA to secure all modes of transportation include "intelligence, regulation, enforcement, inspection, and screening and education of carriers, passengers and shippers" (Bush, 2002:10). By improving the security of transportation systems, which move people to and from the nation's borders every day, the efforts to prevent acts of terrorism in the United States can be greatly enhanced.

2.4.2 Emergency Preparedness and Response

Despite all efforts at preventing terrorist attacks, the United States must be prepared to respond to and recover from incidents that may occur (Bush, 2002:11). Building on the work accomplished by the Federal Emergency Management Agency

(FEMA), the Department of Homeland Security will work to reduce the loss of life and property associated with terrorist attacks by advocating programs focused on preparedness, mitigation, response, and recovery (Bush, 2002:11).

The Department will enhance preparedness by taking control of federal grant programs for state and local first responders and by developing training and evaluation programs for all levels of government (Bush, 2002:11). The Department is to emphasize risk mitigation by supporting the development of communities that have the ability to withstand the consequences of disasters (Bush, 2002:11). The Department intends to improve response efforts by coordinating the national reaction to all forms of terrorist attack and by directing the involvement of other federal response assets (Bush, 2002:11). Finally, the Department is charged to promote recovery from terrorist incidents by minimizing loss of life, health, and property and reducing the fear and panic associated with such incidents (Bush, 2002:11).

2.4.3 Science and Technology

The knowledge, technology, and material needed to build and deliver weapons of mass destruction are far more pervasive than in the past (Bush, 2002:12). Because of this, the Department will employ a division with the sole focus of preparing for and responding to the threat of weapons of mass destruction (Bush, 2002:12). This division is responsible for coordinating the effort to develop national policy, guidelines, exercises, and drills addressing the issue of "catastrophic terrorism" (Bush, 2002:12). A variety of capabilities are involved with this mission.

The Department is working to develop and implement scientific and technological countermeasures to chemical, biological, radiological, and nuclear (CBRN) weapons (Bush, 2002:12). Because human, animal, and plant diseases have surfaced as terrorist weapons, the Department will advocate the research and development of vaccines and antidotes to these threats (Bush, 2002:12). In addition, the Department is working to detect and mitigate attacks involving such weapons (Bush, 2002:12). Further capabilities include the need to prevent the importation of nuclear weapons and materials into the United States (Bush, 2002:13). These capabilities are a vital component in protecting the nation from the CBRN threat.

2.4.4 Information Analysis and Infrastructure Protection

> The Department of Homeland Security would merge under one roof the capability to identify and assess current and future threats to the homeland, map those threats against our current vulnerabilities, inform the President, issue timely warnings, and immediately take or effect appropriate preventive and protective action. (Bush, 2002:14)

Because intelligence is vital to the prevention of terrorism, it is important that terrorist related information is analyzed and disseminated as efficiently as possible (Bush, 2002:14). The new Department plans to systematically analyze all threat information from a variety of sources (Bush, 2002:14). In addition, the Department is taking a more proactive approach to combating terrorism by providing actionable intelligence and warning to those that are responsible for preempting attacks (Bush, 2002:14). In doing so, the Department will be leveraging the increased information gathering capabilities obtained by the FBI to ensure a more complete analysis and warning process (Bush,

2002:14). Overall, the Department will improve the distribution of threat information to all levels of government and the private sector (Bush, 2002:14-15).

Efforts to protect the nation's critical infrastructure are included in the same departmental division as information analysis. Critical infrastructure are "those assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale" (Bush, 2002:15). Though 85 percent of the nation's critical infrastructure is owned by the private sector, the Department of Homeland Security will coordinate a comprehensive national critical infrastructure protection plan to promote security efforts at all levels of government, as well as the private sector (Bush, 2002:15). As part of this planning, the Department will develop and harness all available analytic tools to prioritize protection efforts to ensure that the most significant vulnerabilities are addressed first (Bush, 2002:15). Particularly, the vulnerabilities associated with cyber-based threats will receive a high priority due to the possible cascading effects of such an attack (Bush, 2002:15).

2.4.5 Management

> The final major departmental division is responsible for
>
> budget, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of the Department. (DHS Organization, 2003:np)

The most vital asset of any organization is its personnel. Accordingly, the Directorate of Management is charged with overseeing the activities of the Department's employees and

ensuring their ability to communicate with one another and management (DHS Organization, 2003:np). With responsibility for more than 170,000 personnel, the mission of this division is critical.

2.4.6 Other Key Mission Areas

In addition to the five primary mission areas discussed above, the Department consists of an array of new and existing agencies. Because it is impossible to accomplish all the missions involved with homeland security solely at the federal level, it is vital that the Department work with state and local governments, and the private sector, to address the shared responsibilities of protecting the American people from terrorism (Bush, 2002:16). To accomplish this, the Department includes an Office of State and Local Government Coordination as well as an Office of Private Sector Liaison (DHS Organization, 2003:np).

Three existing agencies, the United States Coast Guard, the United States Secret Service, and the Bureau of Citizenship and Immigration Services, are also incorporated into the Department (DHS Organization, 2003:np). Though the Commandant of the Coast Guard will report directly to the Secretary of Homeland Security, the Coast Guard would operate as an element of the DoD in times of war (DHS Organization, 2003:np). In addition to its mission of protecting the President, Vice President, and other national leaders, the Secret Service has specialized expertise in many other areas, such as counterfeiting, cyber-crime, identity fraud, and access device fraud, that can contribute to the fight against terrorism (Bush, 2002:16). Because of this, the Secret Service will also

report directly to the Secretary of Homeland Security (Bush, 2002:16). Finally, the Bureau of Citizenship and Immigration Services will assist in assuring the provision of efficient immigration services and easing the transition to American citizenship (DHS Organization, 2003:np).

The key mission areas and departmental divisions discussed above incorporate the outline of the vast new government organization being set up by the present administration. Prior to the organization of the Department, more than 100 government organizations had homeland security related responsibilities (Bush, 2002:1). The intention of the Department of Homeland Security is to provide the American people with a "single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future" (Bush, 2002:1). However, as noted by the Hart-Rudman Commission, a new structure would be ineffective without a comprehensive strategy to guide its operations.

2.5 The National Strategy for Homeland Security

In July 2002 the Office of Homeland Security released the nation's first *National Strategy for Homeland Security*. This extensive document sought to better define the homeland security mission by delineating the most important objectives for the Federal government, non-federal governments, the private sector, and American citizens. Thus, its purpose was to "mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks" (National Strategy, 2002:vii).

One of the most significant contributions provided by the Strategy is a complete definition of exactly what "homeland security" entails.

> Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy, 2002:2)

Based on this definition, three fundamental objectives were established for securing the homeland from terrorism. The order in which these objectives are presented deliberately sets priorities for America's efforts (National Strategy, 2002:3).

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism;
- Minimize the damage and recover from attacks that do occur. (National Strategy, 2002:3)

Thus, any set of initiatives targeted at securing the homeland should be firmly grounded on these three concepts.

However, efforts to secure the nation have the potential to negatively impact other facets of American life. Though the United States is at risk for attacks, the mitigation of this risk must be balanced against both economic costs and infringements on individual liberty (National Strategy, 2002:2). The Strategy recognized this need to consider more than just security and emphasized its importance throughout the document. Six critical mission areas were also emphasized that provide focus for homeland security efforts in the future. The first three mission areas focused on the first objective of homeland security, preventing attacks (National Strategy, 2002:viii). The next two mission areas targeted the reduction of vulnerabilities, while the last area focused on minimizing the damage and recovering from attacks that do occur (National Strategy, 2002:viii). Each of these missions is outlined below.

2.5.1 Intelligence and Warning

Because terrorists depend on the element of surprise to successfully execute their attacks, the United States must have an intelligence and warning system that can detect terrorist activities before they manifest into an attack (National Strategy, 2002:15). The lessons learned by the attack on Pearl Harbor in 1941 were applied to Cold War efforts to detect indications of nuclear attacks by the Soviet Union (National Strategy, 2002:15). However, September 11th proved that early warning of terrorist attacks is an extremely difficult and complex mission (National Strategy, 2002:15). The intelligence community must therefore increase its capability to collect and analyze information relevant to homeland security requirements (National Strategy, 2002:17). In addition, the resulting intelligence must be provided to all the pertinent entities so they might take preventive or protective action (National Strategy, 2002:17). Though these capabilities are vital to the security of the nation, they have the potential to affect the basic rights and liberties of American citizens (National Strategy, 2002:15-16).

2.5.2 Border and Transportation Security

Historically, the United States has been able to rely on two vast oceans and two allied neighboring countries for border security (National Strategy, 2002:21). The enhanced capability of modern terrorists to deliver the world's most destructive weapons has, however, forced the nation to adjust its border and transportation security systems (National Strategy, 2002:21). America's borders are fused with the seaports, airports, highways, pipelines, railroads, and waterways that move people and goods in and out of

the country (National Strategy, 2002:21). This fusion has linked virtually every community in the United States to the global transportation network. Accordingly, the Strategy emphasized that the U.S. must

> manage who and what enters our homeland in order to prevent the entry of terrorists and the instruments of terror while facilitating the legal flow of people, goods, and services on which our economy depends. (National Strategy, 2002:22)

This will include work with the international community and the private sector to secure the transportation systems that convey people and goods to the nation's borders (National Strategy, 2002:22).

2.5.3 Domestic Counterterrorism

The events of 9/11 have required federal, state, and local law enforcement agencies to reprioritize their efforts to emphasize the prevention and interdiction of terrorist activity within the United States (National Strategy, 2002:25). This adjustment necessitates the enhanced sharing of information among intelligence agencies and international, federal, state, and local law enforcement (National Strategy, 2002:25). To be effective, the Strategy states that information pertaining to the financial and logistical support for terrorist activity must be more effectively disseminated across all levels of law enforcement (National Strategy, 2002:26). Through this coordination and information sharing, the law enforcement community as a whole will be better equipped to "identify, halt, and, where appropriate, prosecute terrorists in the United States" (National Strategy, 2002:26).

2.5.4 Protecting Critical Infrastructure and Key Assets

The three mission areas described in Sections 2.5.1. – 2.5.3. focus primarily on efforts to prevent terrorist attacks within the United States. The mission described here, as well as the subsequent mission area, focus on efforts to reduce America's vulnerability to attack. The opportunistic nature of terrorism suggests that terrorists "exploit vulnerabilities we leave exposed, choosing the time, place, and method of attack according to the weaknesses they observe or perceive" (National Strategy, 2002:29). Increasing the security of one target may only shift the terrorist's interests to another. Thus, it is infeasible to completely protect every potential target in America (National Strategy, 2002:29). However, by making strategic improvements to the protection and security of the nation's *critical* infrastructure and *key* assets, terrorist attacks can be deterred, deflected, or their effects mitigated (National Strategy, 2002:29).

Consistent with the USA PATRIOT Act, the Strategy defines critical infrastructure as:

> Those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (National Strategy, 2002:29-30)

Critical infrastructure sectors identified by the Strategy include agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, and postal and shipping (National Strategy, 2002:30). The protection of these sectors will require "an unprecedented level of cooperation throughout all levels of government, with

private industry and institutions, and with the American people" (National Strategy, 2002:31).

2.5.5 Defending against Catastrophic Threats

The capability of terrorists to acquire and deliver chemical, biological, radiological, and nuclear weapons is proliferating at a rapid pace (National Strategy, 2002:37). Because the consequences of an attack with these weapons of mass destruction could easily be far more devastating than those suffered on 9/11, the United States must enhance its capability to detect and respond to catastrophic threats (National Strategy, 2002:37). The Strategy noted a lack of coordination and cooperation among federal, state, and local response mechanisms as a major stumbling block in times of severe crisis (National Strategy, 2002:37-38). America must "have a coordinated national effort to prepare for, prevent, and respond to chemical, biological, radiological, and nuclear terrorist threats to the homeland" (National Strategy, 2002:38). To accomplish this, the U.S. intends to consolidate and synchronize the pervasive efforts of multiple federal agencies and organizations (National Strategy, 2002:38).

2.5.6 Emergency Preparedness and Response

While the previous five mission areas focused on the first two objectives of homeland security, this final critical mission targets the need to minimize the damage and recover from any future attacks that may occur. The Strategy stated that preparedness efforts are key to providing an effective response (National Strategy, 2002:41). The

nation must plan, equip, train, and exercise an array of response assets in the development of a comprehensive, coordinated national system (National Strategy, 2002:41). America's nearly three million state and local first responders – police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials – provide a strong basis for such a system (National Strategy, 2002:41). In times of catastrophic emergency the Federal government will need to augment state and local efforts (National Strategy, 2002:41). The United States needs a "fully integrated national emergency response system that is adaptable enough to deal with any terrorist attack, no matter how unlikely or catastrophic…" (National Strategy, 2002:42).

2.5.7 The Foundations of Homeland Security

The National Strategy also delineates four unique American strengths that cut across all mission areas (National Strategy, 2002:x). Law, science and technology, information sharing, and international cooperation all provide a useful framework for evaluating federal investments in homeland security (National Strategy, 2002:x). New legislative actions (i.e. law) could help enable the U.S. to fight terrorism more effectively, but should avoid incursions on the freedoms of its citizenry (National Strategy, 2002:x). New technologies for analysis and dissemination of information, and detecting and countering attacks involving weapons of mass destruction would help to prevent and minimize the damage of future terrorist incidents (National Strategy, 2002:xi). The sharing of information among databases used for federal law enforcement, immigration,

intelligence, public health surveillance, and emergency management contributes to every aspect of homeland security (National Strategy, 2002:xi). Finally, because modern terrorists pay no respect to traditional boundaries, America must pursue an international agenda to counter the global threat of terrorism (National Strategy, 2002:xii). These foundations cut across all levels of government and across all sectors of society in their contribution to homeland security objectives (National Strategy, 2002:x).

The *National Strategy for Homeland Security* provides a significant basis for future initiatives and planning in the effort to combat terrorism within the United States. The definitions, objectives, and mission areas delineated within its pages contribute a great deal to the standardization of homeland security thinking. For this reason, this thesis leverages the Strategy more than any other source in the development of a value-based decision-making tool.

2.6 ANSER Institute for Homeland Security

The ANSER Institute provides a variety of resources and commentary regarding the security of the United States homeland from terrorism. In particular, the Institute advocates the consideration of a seven element "Strategic Cycle" in the development of homeland security strategy, policy, and resource allocation (ANSER, 2002:1). Figure 2-2 displays this logical cycle.

Figure 2-2: ANSER Institute Strategic Cycle

The Institute states that the primary preference is the *deterrence* of terrorism (McIntyre, 2001:np). Deterrence is based on the terrorist's perceived punishment for their actions and the denial of the effects they seek (ANSER, 2002:1). However, efforts to instill fear of punishment and failure take time (McIntyre, 2001:np). Any failure at deterrence will require working through the full cycle to restore deterrence (McIntyre, 2001:np).

Whether efforts at deterrence fail, or the enemy is simply undeterable, the United States will have to rely on *prevention* capabilities (ANSER, 2002:1). Prevention involves an array of both passive and active measures aimed at mitigating or even stopping an attack or its effects (ANSER, 2002:1). These defensive activities range from arms control treaties to border control and law enforcement (ANSER, 2002:1).

Given sufficient intelligence, the nation must have the capabilities and associated policies that allow for the *preemption* of imminent attacks (McIntyre, 2001:np, ANSER,

2002:1). Unfortunately this is a policy filled with political and military risks both at home and abroad (ANSER, 2002:1). Regardless, to assure the defense of the homeland the United States must use all elements of national power to preempt terrorists before they can carry out attacks (ANSER, 2002:1).

If the U.S. should fail to deter, prevent, or preempt attacks, the Institute states that the capability for *crisis management* must exist. This effort includes the investigation and law enforcement response to imminent or actual attacks within the United States (ANSER, 2002:2). Crisis management involves the coordination of activities at every level of government focused on containing and minimizing the impact of the attack while providing immediate aid to those affected (ANSER, 2002:2). These efforts continue until the current incident has come to a close (McIntyre, 2001:np).

Following an attack, the Institute notes that emergency relief services must be provided to governments, businesses, and individuals and vital systems must be restored (ANSER, 2002:2). Though the majority of this responsibility is held at the local level, *consequence management* will involve an equal amount of government coordination and cooperation (McIntyre, 2001:np). In the event of catastrophic terrorist attacks, federal assistance will be vital (ANSER, 2002:2).

The key to ensuring that the individuals responsible for an attack are brought to justice is *attribution* (McIntyre, 2001:np). The efforts of intelligence and law enforcement entities must be applied to removing the anonymity that provides security for terrorists (McIntyre, 2001:np, ANSER, 2002:2). In addition, the case must be sound enough to support a conviction in the court of public opinion (McIntyre, 2001:np). Sufficient attribution is required to employ a strategic response (ANSER, 2002:2).

The *response* to a terrorist attack must not only eliminate the current threat, but also restore the deterrence necessary to ward off future attacks (ANSER, 2002:3). The Institute states that the United States could accomplish these goals through arrests and prosecutions, or by treating the attributed individuals as military targets (McIntyre, 2001:np). The choice of response would be dependent on an array of factors, including the origin of the attacker (ANSER, 2002:3).

The ANSER Institute further utilizes their seven-step cycle, along with six significant methods of attack that terrorist threats might employ, to define mission areas that the United States must have the capability to execute. Chemical, biological, radiological, nuclear, cyber, and enhanced conventional attacks threaten the vital interests and even the survival of the nation (Larsen, 2002b:np). All levels of government, as well as the private sector, must therefore perform the 42 mission areas displayed in Table 2-1 in order to secure the homeland from terrorism (Larsen, 2002b:np).

Table 2-1: Homeland Security Mission Areas

	Deterrence	Prevention	Preemption	Crisis Management	Consequence Management	Attribution	Response
Chemical							
Biological							
Radiological							
Nuclear							
Cyber							
Enhanced Conventional							

MISSION AREAS

(Larsen, 2002b:np)

The Institute recommends that the nation combat terrorism by "planning, organizing, training, equipping and exercising to be as strong as possible in each of the mission areas" (Larsen, 2002b:np).

2.7 Value Focused Thinking

Efforts to secure the American homeland from terrorism require a variety of difficult decisions. To ensure that these decisions are made in the most beneficial manner, an effective decision-making methodology is required. Value Focused Thinking (VFT) provides such a methodology. The remaining sections of this chapter review the principles of VFT and the benefits of applying it to a decision-making process.

2.7.1 Decision-Making

As pointed out by Kirkwood, "the one essential element of a decision is the existence of alternatives" (Kirkwood, 1997:2). If there are not multiple options to think about, then there truly is no decision to consider. Given the array of strategies and preferences that could be pursued in securing the homeland, a very difficult decision problem does indeed exist. Four basic sources of difficulty in decision-making are the complexity of the decision, the uncertainty of the situation, the existence of multiple competing objectives, and conflicting perspectives from multiple stakeholders (Clemen, 2001:2). Complicating the process further is the fact that, in most decision problems, various alternatives can lead to dissimilar outcomes (Kirkwood, 1997:2). Unfortunately, the homeland security decision context suffers from all of these difficulties.

Given these complications it is vital that important decisions are made strategically. That is, decisions should be made skillfully "in a way that is adapted to the ends we wish to achieve (Kirkwood, 1997:3). According to the DoD definition of strategy, this would mean making decisions in a "synchronized and integrated fashion to achieve theater, national, and/or multinational objectives" (JP 1-02, 2001:417). When cast in the context of homeland security, a strategy will need to be a synchronized and integrated approach to achieve local, state, federal, and international objectives. VFT provides a strategic methodology that is well suited to addressing the various difficulties associated with making tough decisions.

2.7.2 Thinking About Values

"Values are what we care about." (Keeney, 1992:3)

The usual method for decision-making involves selecting a solution from an available set of alternatives (Keeney, 1992:3). Keeney refers to this as Alternative Focused Thinking (AFT) (Keeney, 1992:4). Indeed, most decision processes begin with a list of the possible solutions, ranking them from the best to the worst, and selecting the "optimal" alternative (Keeney, 1992:4). However, the specific alternative is chosen to gain specific benefits and avoid undesirable consequences; the selection is based on *values* (Keeney, 1992:3). Thus, "alternatives are the means to achieve the more fundamental values" (Keeney, 1992:3). Rather than starting with alternatives and evaluating which one is preferred, VFT begins with defining the best possible option and works toward making it a reality (Keeney, 1992:6).

The five steps identified by Keeney in this process are:

- Recognize a decision problem
- Specify values
- Create alternatives
- Evaluate alternatives
- Select an alternative. (Keeney, 1992:49)

The fundamental difference between this VFT process and that for AFT is that values are identified directly after a problem has been realized, whereas AFT defines the alternatives before the values (Keeney, 1992:49). With VFT, the creation of alternatives can be based on and tailored to what is important to the decision context and not simply focus on previously identified alternatives (Keeney, 1992:50). In turn, the evaluation and selection of an alternative will be more accurately rooted in the decision-maker's values (Keeney, 1992:50).

Keeney points out a variety of advantages that can be gained by thinking about values (Keeney, 1992:24). These key outcomes from the use of VFT are:

- Uncovering hidden objectives
- Guiding information collection
- Improving communication
- Facilitating involvement in multiple-stakeholder decisions
- Avoiding conflicting decisions
- Evaluating alternatives
- Creating alternatives
- Identifying decision opportunities
- Guiding strategic thinking (Keeney, 1992: 24-27).

All of these benefits are products of a decision-making methodology based on thinking about values. Keeney maintains that VFT provides a much more robust method for not only solving recognized problems, but for uncovering problems that may exist in the future (Keeney, 1992:47). In fact, many of the advantages described above have no obvious counterpart in an alternative-based methodology (Keeney, 1992:48).

The superiority of VFT over AFT was demonstrated in a study performed by Professor G. Leon Orfelio at the University of Madrid. His research intended to "discover whether the structure of objectives generated with value-focused thinking (VFT) is different from the structure generated with alternative-focused thinking (AFT)" (Orfelio, 1999: 213). The two-part study surveyed a total of 58 psychology students, 28 of which had 80 hours of training in decision analysis, to ascertain if a) differences exist between the structures of objectives generated with the two methods, and b) if VFT is the superior method based on various criteria (Orfelio, 1999:215,223). The first study found that the VFT approach generated a wider array of objectives, was more hierarchical, and provided more metrics for assessing the alternatives (Orfelio, 1999:224). All of these properties are beneficial to a strategic decision-making process. The second study found that the utilization of the VFT structure developed in the first study, rather than the AFT, assisted in the development of a much more robust set of alternatives (Orfelio, 1999:225). Overall, the research performed by Professor Orfelio showed that, compared to AFT, "VFT is more complete, more operational, equally concise, and more understandable" (Orfelio, 1999:225). These characteristics result in a decision-making process that is superior to processes that focus primarily on alternatives.

Orfelio's study demonstrates that VFT is an extremely beneficial and effective method for analyzing and supporting decision-making in a variety of venues. Homeland security is no exception. However, before VFT is applied to the subject of this research it may be advantageous to examine a number of successful applications in other fields. Keefer, Corner, and Kirkwood describe the use of VFT throughout the 1990's in the energy industry, manufacturing and services community, medical field, and the military

by reviewing 57 application articles in operations research journals (Keefer, 2000:5-6). Two significant, national security related applications of VFT are summarized below.

2.7.3 Applications of VFT

SPACECAST 2020

In May 1993 the Chief of Staff of the Air Force directed Air University to conduct a study to ascertain the space capabilities, and supporting technologies, the United States would need to pursue in order to preserve national security into the 21st century (SPACECAST 2020: Executive Summary, 1994:4). The 10-month effort, titled SPACECAST 2020, incorporated the expertise of a multitude of students, scientists, technologists, and operators in both military and civilian organizations (SPACECAST 2020: Executive Summary, 1994:4). In the face of limited resources, it was deemed necessary to prioritize space initiatives, in order to maximize operational effectiveness, once capabilities and technologies had been identified (SPACECAST 2020: Operational Analysis, 1994:5). To accomplish this goal, the analysis team chose VFT as the most appropriate methodology (SPACECAST 2020: Operational Analysis, 1994:5).

In order to evaluate the various space-related systems (i.e. capabilities) the team utilized the draft JCS Pub 3-14, "Military Space Operations Doctrine," to develop a value hierarchy of the fundamental objectives guiding space operations (SPACECAST 2020: Operational Analysis, 1994:7). This method of deductively developing the value hierarchy from previously established strategic objectives, visions, and doctrine is known as the "Gold Standard" (Parnell, 2002). Using this technique, the control and exploitation

of space were identified as overall objectives while *force enhancement*, *force application*, *space control*, and *space support* were recognized as upper level means for achieving these goals (SPACECAST 2020: Operational Analysis, 1994:7). Using these objectives as the upper two tiers in the hierarchy sub-objectives were developed until measures could be created to rank the various systems (SPACECAST 2020: Operational Analysis, 1994:8).

The VFT analysis allowed the team to answer two fundamental questions regarding future space operations.

- Which of the SPACECAST 2020 system concepts offer the greatest promise of increasing operational effectiveness?
- What are the technologies offering the greatest leverage in turning high-value system concepts into operational realities? (SPACECAST 2020: Operational Analysis, 1994:5).

The results of the SPACECAST 2020 study were widely accepted as they produced an array of new ideas while reinforcing old ones (Keefer, 2000:22, SPACECAST 2020: Executive Summary, 1994:20). Overall, the study confirmed the applicability of VFT to identifying objectives and developing future national security priorities.

Air Force 2025

In 1995 the Chief of Staff of the Air Force tasked Air University to perform a study, called *Air Force 2025*, that would specify the capabilities the United States would need to establish and maintain air and space dominance thirty years into the future (Jackson, Jones, and Lehmkuhl, 1996:vii). It was necessary for the study team to identify the desired objectives and supporting technologies in a way that was "objective,

traceable, and robust" (Jackson *et al*, 1996:vii). After considering a variety of possible methodologies to complete this task, the team selected VFT as the most useful means for achieving their goal (Jackson *et al*, 1996:6). Its successful utilization in the *SPACECAST 2020* study was a contributing factor to the selection of VFT for *Air Force 2025* (Jackson *et al*, 1996:6, Keefer, 2000:21).

In constructing the value model, the team leveraged the knowledge of a variety of experts in both the military and civilian world (Jackson *et al*, 1996:5). Through VFT the team was able to identify *awareness, reach, and power* as the fundamental objectives for achieving air and space dominance (Jackson *et al*, 1996:14). These values, and the subsequent sub-values, were formed into a hierarchical structure that allowed the team to evaluate the implications of pursuing a variety of technological systems in the future. This evaluation allowed the team to rank order the candidate systems and determine the required high-leverage technologies to support them (Keefer, 2000:23).

In the end, *Air Force 2025* was assessed as the "starting point for Value Focused Thinking with the Department of Defense" (Jackson *et al*, 1996:43). The applicability of the *2025* value model as a framework for future air and space doctrine was also noted (Jackson *et al*, 1996:43). VFT was a very useful tool in the assessment of future needs to ensure air and space superiority.

While these studies are only two examples of the use of VFT in major analyses, they highlight the successful use of VFT for complex national level decisions of critical impact. In the face of the complex challenges of homeland security, VFT presents an extremely useful method of analysis to support decision-making.

2.8 Summary

The problem facing homeland security decision-makers is complex and pervasive. Early studies delineated an array of steps that would be necessary to combat the threat of terrorism to the United States homeland. The clear definition of homeland security objectives, the development of a national strategy, and the establishment of a federal agency with homeland security as its primary mission were all recognized as minimum requirements. Sadly, these recommendations were not fully taken note of until after 9/11. Now that homeland security is widely acknowledged as one of the most fundamental missions of the Federal government, plans, policies, and actions must be developed and implemented to combat terrorist threats and attacks within the United States. The decision of which plans, policies, and actions to pursue is a difficult one. A sound decision-making methodology is needed in order to identify the most beneficial strategy to secure the homeland. Value Focused Thinking has been successfully applied to similar decision problems and will yield equal benefits to homeland security. Chapter 3 further outlines the VFT process and establishes the knowledge base necessary to apply the methodology to the subject of this research.

3. The Value-Focused Thinking Process

Chapter 3 delineates the Value Focused Thinking (VFT) methodology utilized in this research. In particular, the problem facing homeland security decision-makers is clearly defined and the development of a value hierarchy, evaluation measures, and single dimension value functions is discussed. The actual application of this methodology to homeland security is presented in Chapter 4.

3.1 Introduction

In applying the VFT methodology, it is vital that the value hierarchy be properly based on the problem of interest. If the problem is not appropriately identified, the subsequent value model and analysis may not address the fundamental question at hand. In terms of this research, the problem of securing the homeland from terrorism is incredibly complex. Thus, the first step presented in this chapter clearly delineates the problem facing homeland security decision-makers.

Once the problem is identified, the VFT methodology dictates that the issues of importance (or value) must be identified, clarified, and organized into a hierarchical structure. Section 3.3. discusses various guidelines and methods for developing a value hierarchy. In particular, the affinity diagramming method, which is utilized in this research, is introduced.

When values have been recognized and structured, some method for assessing the attainment of those values is needed. Accordingly, the third step performed in this

research is the development of evaluation measures. The various types and characteristics of evaluation measures are discussed in Section 3.4., while Chapter 4 presents the specific measures developed for this research.

Finally, in order to implement an evaluation measure, it is necessary to construct a single dimension value function (SDVF) that assigns a score to each alternative homeland security strategy. Because various values will require dissimilar measurements, an overall scoring requires the attainment of values to be standardized to a single scale. A SDVF accomplishes this need. The fourth and final step in the methodology performed for this research addresses an array of SDVFs that can be applied to value hierarchies.

Because of the magnitude of the problem and the resources and personnel available to complete the study, this thesis effort is focused on the initial stages of a VFT analysis. The next logical step, beyond what is completed in this research, would be to weight the various values contained in the hierarchy. This process accounts for the possibility of dissimilar levels of importance among varying values. Unfortunately, it is also critically dependent on the expertise and authority of decision-makers at the appropriate level of authority. Weights should be determined by the highest-level decision-maker responsible for the relevant area. Though the weighting process is beyond the scope of this research, Appendix A contains an overview of weighting concepts to facilitate its eventual accomplishment.

3.2 Problem Identification

As was discussed in Chapter 1, the threat of terrorism in the United States is on the rise. The motivation and capabilities of modern terrorists, coupled with the pervasive vulnerabilities of the nation's critical infrastructure and key assets, present a multitude of significant challenges. To meet these challenges, it is necessary to develop and evaluate effective strategies for securing the United States and its citizens from terrorist acts. Currently, there appears to be *no* broad-based, overarching structure, value model or not, for developing and evaluating such strategies. The development of such a structure requires a thorough understanding of what is critical in securing the homeland.

The Preamble of the United States Constitution not only defines the basic purpose of our federal government, but also clearly identifies the key issues in homeland security. The Preamble states:

> We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution for the United States of America. (Constitution, 2002:np)

Though providing for the common defense is generally recognized as a homeland security requirement, the remaining stipulations of the Preamble apply as well. A closer examination of our government's highest responsibilities assists in identifying the value trade-offs that are at the root of the homeland security problem.

In addition to providing for the common defense, a complete security strategy would incorporate all of the responsibilities described in the Preamble. Such a strategy would establish justice by identifying the perpetrators of terrorist acts and ensuring that

they are appropriately punished for their crimes. This would be done, however, in a manner that assures justice to the innocent as well as the guilty. The need to identify the enemy (attribution) and to respond with either law enforcement or military force (response) has been acknowledged (ANSER, 2002:2-3). However, this response must also ensure justice for those accused by not denying them the legal rights promised by law. It remains a premise of U.S. jurisprudence that the accused is assumed to be innocent until proven guilty. A comprehensive strategy would also assist in ensuring domestic tranquility by deterring and preventing terrorist acts that aim to disrupt the peace of the nation. It would promote the general welfare by properly training and equipping first-responders, governments, and the citizenry to react to the most dire situations, for example. Finally, a complete homeland security strategy secures the blessings of liberty for the citizens of the United States by minimizing the impact on personal freedoms and civil liberties while providing the security necessary to nurture freedom. All of these values must be weighed and balanced against one another in the development of homeland security strategy.

However, unlike justice for victims, tranquility, defense, and welfare, which are positively correlated with increases in homeland security, justice for those accused and individual liberties may be negatively impacted as the nation becomes more secure. In a 2001 article, "Countering Terrorism: The Clash of Values," Keeney provided the following example of how security impedes freedom:

> Aware of a threat of bridge destruction, an individual must balance his or her loss of freedom and inconvenience of not using the bridge against the potential safety consequences of using it. The state of California on Nov. 11 stopped and searched all large trucks before allowing them to cross the Golden Gate Bridge. This inconvenienced and reduced the freedom of

> truckers and increased the potential safety of all bridge users. (Keeney, 2001:2)

Thus, value trade-offs between security, which inherently includes justice for victims, tranquility, defense, and welfare, and the rights of victims and the freedoms of America's citizens truly exemplify the problem facing homeland security decision-makers.

In addition, the allocation of resources, financial and otherwise, must be considered in the strategy development process. Given an unlimited quantity of resources, the homeland might be secured. Even if unlimited resources were available, however, actions that would totally secure the nation could quite likely incur an unacceptable reduction in personal freedom. The *National Strategy* acknowledges the trade-offs involved in combating terrorism, recognizing the need to "constantly balance the benefits of mitigating this risk against both the economic costs and infringements on individual liberty that this mitigation entails" (National Strategy, 2002:2).

Clearly, the problem facing homeland security decision-makers involves consideration of the value trade-offs concerned with securing the homeland, avoiding excessive economic and resource costs, and minimizing the impact on personal freedoms and civil liberties. In particular, this research addresses these homeland security issues at the *national executive level*. Thus, the objective of this research, to develop a value hierarchy for homeland security, focuses solely on the values and responsibilities at the *federal* level. While the state, local, and citizen levels are all critical to the security of the homeland, this initial effort has focused on the federal level. Ideally, further studies will develop these other areas in an integrated manner.

The hierarchy of security objectives is complemented by two additional hierarchies that consider the resource and civil liberty costs associated with the security strategy of interest. This three-hierarchy approach was successfully utilized in the development of a value model for information assurance (IA), and could potentially be equally beneficial to the homeland security decision problem (Hamill, 2000, Beauregard, 2001).

Given the clear delineation of the decision problem, a value hierarchy must be created.

3.3 Creation of Value Hierarchy

In framing a decision it is necessary to develop a complete understanding of the *decision context* and the *fundamental objectives* (Keeney, 1992:30). "The decision context defines the set of alternatives appropriate to consider for a specific decision situation" (Keeney, 1992:30). The decision context of this research entails varying strategies for securing the homeland. Evaluation of these strategies requires an understanding of the fundamental objectives concerning homeland security decision-makers. Keeney points out the following regarding fundamental objectives:

> Values of decisionmakers are made explicit with objectives. Hence, the set of objectives developed for a decision frame is absolutely critical. The fundamental objectives are the basis for any interest in the decision being considered. These objectives qualitatively state all that is of concern in the decision context. They also provide guidance for action and the foundation for any quantitative modeling or analyses that may follow this qualitative articulation of values. (Keeney, 1992:33-34).

Therefore, in applying a value-focused decision analysis methodology it is imperative that the pertinent objectives be identified. In addition to determining what is important, it is necessary to identify "how to measure how well the various decision alternatives perform with respect to the 'important things'" (Kirkwood, 1997:11). It is this need to measure alternatives, in part, which leads to the creation of a value hierarchy.

The structuring of objectives into a hierarchical model affords a variety of advantages to the decision process. In general, this structure "improves our understanding of the values that matter, leads to a better value model, and enhances the quality of the value-focused thinking" (Keeney, 1992:86). Further benefits provided by a hierarchical structure include,

- Higher-level objectives assist in the specification of lower-level objectives;
- Helps identify missing or unrecognized objectives;
- Avoids redundancy in the determination of objectives;
- Lower-level objectives, once specified, are easier to measure than upper-level objectives;
- The measurement of lower-level objectives indicates the degree of attainment of upper-level objectives. (Keeney, 1992:86-87).

It is not enough to merely recognize the objectives associated with a particular decision problem; these objectives must be organized into a hierarchical structure if the alternatives related to the decision context are to be accurately measured.

3.3.1 Characteristics of a Value Hierarchy

When discussing the mechanics of developing and utilizing a value hierarchy, there are a few key terms that must be defined. The horizontal levels of a hierarchy are referred to as *tiers*. As one tier of objectives is further specified, a new tier is developed.

The vertical sections of a hierarchy, all tied to the same parent node, are referred to as *branches*. For any particular objective, all of the lower level objectives and measures that fall below it incorporate a branch. Figure 3-1 displays a tier and branch for a simple hierarchy.

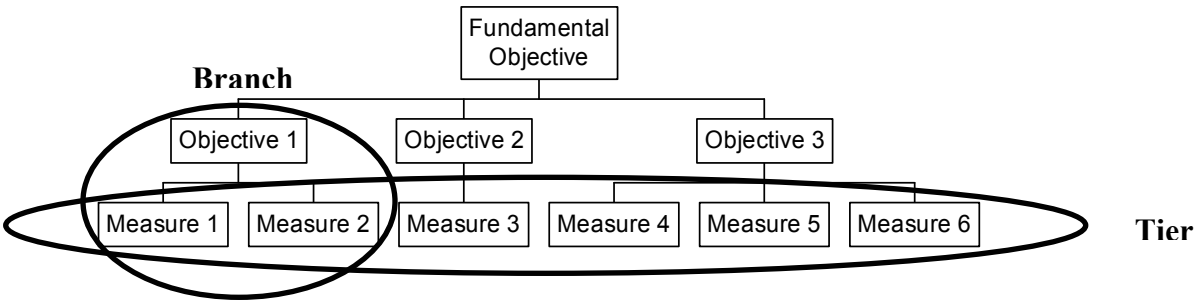

Figure 3-1: Sample Hierarchy

Value hierarchies should be designed to comprise a few key properties. These properties include completeness, nonredundancy, decomposability, operability, and small size (Kirkwood, 1997:16). Each of these properties is briefly described in the remainder of this section.

Completeness

For a value hierarchy to be complete, the objectives expressed at each tier, taken as a whole, must adequately incorporate all relevant factors necessary to evaluate the overall objective of the decision (Kirkwood, 1997:16). For this research, a complete value hierarchy will include all concerns at the federal level necessary to evaluate alternative strategies for securing the homeland from terrorism. The property of completeness is often referred to as collectively exhaustive.

Nonredundancy

For a value hierarchy to be nonredundant, no two values in the same tier should overlap (Kirkwood, 1997:16-17). Because each tier of a hierarchy breaks down, or

clarifies, the values in the tier above it, there should be no "double counting" of objectives (Kirkwood, 1997:17). If the values in one branch of a particular tier are nonredundant, then those values are said to be mutually exclusive.

In decision analysis, it is not only desired, but required that value hierarchies be collectively exhaustive and mutually exclusive (Kirkwood, 1997:17). If a hierarchy is not complete, then alternatives will not be scored according to all that is truly important to the decision-maker. If the hierarchy is redundant, then certain values may artificially receive more weight than was intended. Thus, these two properties are vital to the development of an accurate value model.

Decomposability (Independence)

For a value hierarchy to be decomposable, the value attached to variations in the scoring of objectives on each tier must be independent of the scoring of the other objectives on that tier (Kirkwood, 1997:18). As an example, Kirkwood points out decomposability problems when a job seeker considers three economic issues; salary, pension benefits, and medical coverage (Kirkwood, 1997:17). If the job has very good pension benefits, then an increase in salary may not receive as much value as if the job seeker has to provide for their own retirement out of his or her salary (Kirkwood, 1997:18). Values such as these are not decomposable. For this problem, assigning equivalent dollar values to salary, pension benefits, and medical coverage and combining these concerns into a single economic issues measure can overcome decomposability problems (Kirkwood, 1997:18).

Operability

For a value hierarchy to be operable, it must be "understandable for the persons who must use it" (Kirkwood, 1997:18). This issue often arises when technical specialists present their work to the general public (Kirkwood, 1997:18). The use of unnecessarily complex terms and measures should be avoided if the value hierarchy is to be presented to and utilized by persons unfamiliar with such terminology. It is important that the hierarchy is developed with the ultimate decision-maker (or decision-makers) in mind.

Small size

For a value hierarchy to be considered small, it must be more easily communicated and require fewer resources to estimate the performance of alternatives than an equivalent hierarchy with a greater number of objectives (Kirkwood, 1997:18). It can be difficult to balance between ensuring the hierarchy is complete and being able to finish the analysis in a finite time period (Kirkwood, 1997:19). The quest for completeness may lead to a hierarchy that is too complex to be operational. Keeney and Raiffa offer the following advice regarding how far down to specify a hierarchy.

> Our judgment must be used to decide where to stop the formalization by considering the advantages and disadvantages of further specification. If this were not done, and the hierarchy were carried to absurd lengths, we would end up with an astronomical set of objectives…the point of all this is that we must be pragmatic about the level of detail or specification we are prepared to assess. (Keeney and Raiffa, 1976:43)

The question of how far to extend the hierarchy is largely dependent on who the decision-maker is and what they intend to use the hierarchy for (Keeney and Raiffa, 1976:43). Because this study focuses on federal level homeland security decision-making, the hierarchy should not be specified to too fine a level of detail. Additionally, the hierarchy

should only include those objectives that are truly of interest at this level of decision-making.

This difficulty can be overcome by performing the "test of importance" to ascertain what objectives should be included (Kirkwood, 1997:19). This test states that an objective should only be included in the hierarchy if "possible variations among the alternatives with respect to the proposed [objective] could change the preferred alternative" (Kirkwood, 1997:19). When the alternatives are not clear, as is the case in this research, the relevant literature must be relied on to determine what is important. Regardless, the "test of importance" assists in the effort to keep the value hierarchy as small as possible. Given the properties stated above, the value hierarchy must now be constructed.

There are two *primary* ways in which a value hierarchy can be constructed. The decision of which method to utilize is largely based on how well alternative solutions are defined (Kirkwood, 1997:20). With clearly defined alternatives, the hierarchy can be developed by first identifying evaluation measures and then grouping these measures into higher-level objectives (Kirkwood, 1997:20). This method is known as a *bottom-up* approach. However, with this research it is not clear what alternative strategies for homeland security will entail. Thus, it is necessary to use a *top-down* approach. "In situations where the alternatives are not well specified at the start of the analysis, an approach starting with the overall objective and successively subdividing objectives is more appropriate" (Kirkwood, 1997:20). By using the *top-down* approach, this research begins with the overall objective of securing the homeland and specifies lower level objectives for accomplishing this goal. This development is based on the literature

reviewed in Chapter 2. By identifying key objectives from doctrinal literature, this research utilizes the same "Gold Standard" method employed in SPACECAST 2020. The subsequent organization and specification of these objectives is accomplished through a process known as *affinity diagramming*.

3.3.2 Affinity Diagramming

In some cases, it can be difficult to obtain a complete value hierarchy when applying the top down method. With this research, the homeland security decision environment is evolving and spans a vast and complex space. Because of this, lower tier objectives are difficult to define. This roadblock suggests that some form of bottom up analysis, in conjunction with the top down specification, may benefit the pursuit of a collectively exhaustive hierarchy. Affinity diagramming offers one such method for furthering the development of the value hierarchy.

Affinity diagramming is a technique for gathering "large amounts of ideas, opinions, issues, etc. and [organizing] them into groupings based on the natural relationship (affinity) between the items" (Area, 2002:np). This decision-making process arranges ideas into a hierarchical structure that can be very useful in identifying common themes among a vast array of concepts (Bureau, 2002:np, Texas Tech, 2002:np). Affinity diagramming not only helps to delineate all the factors in a given decision problem, but the subsequent groupings become the basis for strategies to solve the problem (U. of Mass., 2002:np). By breaking down complicated issues into broad categories, this

technique provides structure to convoluted problems that have no clear solutions (CERN, 2002:np).

There are a variety of situations in which affinity diagramming can be useful. It is applicable when facts are disorganized and uncertain and need to be arranged in a systematic manner (Texas Tech, 2002:np). It can also be used "when the issues being investigated are numerous and complex, and the thoughts on how to deal with the issues are in disarray" (U. of Mass., 2002:np). Finally, affinity diagramming is an appropriate technique when the problem necessitates the involvement and support of a group (Area, 2002:np). Clearly all of these situations, in varying degrees, apply to developing a homeland security value hierarchy.

A number of institutions have developed steps for creating an affinity diagram. The majority of the discrepancies between alternative processes stem from the level of detail used. By combining the broad concepts shared by many of these previously developed processes, a general method for constructing an affinity diagram is established. The following steps provide this method.

- Clearly define the problem or issue under consideration
- Research and record issues and ideas pertaining to the problem
- Collect all ideas together and randomize them
- Organize the collection of ideas into related groups
- Label related groups according to the specific theme
- Discuss and confirm the groupings

These steps are a very general method for accomplishing this technique. More detailed instructions should be left to the individual facilitating the creation of the affinity diagram.

The affinity diagramming technique has been utilized in a variety of circumstances where problems and issues were poorly defined. The Technical Support Division of the European Organization for Nuclear Research provide an example of how affinity diagramming was used to identify obstacles in implementing Total Quality Management (TQM) in an organization (CERN, 2002:np). In this small example, 36 group-generated thoughts were categorized into eight overarching concepts that facilitated the development of solutions (CERN, 2002:np).

A more defense-oriented application of affinity diagramming can be found in the development of the value model for Air Force 2025 (Jackson *et al*, 1996). In this case, the analysis team organized 109 air and space tasks into 14 mutually exclusive, collectively exhaustive task groupings (Jackson *et al*, 1996:1). Once these 14 groupings were appropriately labeled, the team was able to fashion the tasks and subtasks into a hierarchical structure that became the *Foundations 2025* value model (Jackson *et al*, 1996:6). As was described in Chapter 2, the development of this model as part of the Air Force 2025 study provided significant insight into the future needs of the United States Air Force.

Thus, the use of affinity diagramming for organizing and defining complex issues can be truly beneficial in a vast array of applications. Homeland security is no exception. By clearly and completely delineating and grouping all of the issues concerning the security of America, as outlined in various resources, affinity diagramming provides an exceptional method for performing a bottom up completion and validation of a top down value hierarchy.

For this research, the issues and initiatives pertaining to homeland security were obtained from the literature. In particular, a content analysis was performed on the following five prominent homeland security documents to obtain a vast collection of ideas and concepts (Stemler, 2001).

- *The National Strategy for Homeland Security*, released by the Office of Homeland Security
- *The Department of Homeland Security*, released by President Bush
- *Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council*
- *Securing the Homeland Strengthening the Nation*, budget released by President Bush
- *Homeland Security: The Strategic Cycle*, released by the ANSER Institute for Homeland Security

This analysis led to the extraction of **363 objectives** related to securing the homeland from terrorist threats and attacks. Using this collection of homeland security objectives, common themes and issues were grouped together to form a hierarchical structure. The sub-objectives were first grouped according to the three objectives included in the National Strategy's definition of homeland security (Prevention, Vulnerability Reduction, Response Preparedness). Each of these groups was further sub-grouped in order to validate and in some cases supplement the doctrine-based definition. The complete listing of these objectives, as they were grouped, is presented in Appendix B along with their sources. This method not only assists in the completion of the value hierarchy, but also provides quantifiable support for the values that are included. The hierarchy that resulted from this technique is discussed in Chapter 4.

Thus, the structuring of fundamental objectives into a value hierarchy is a vital step in the VFT process. The hierarchical structure not only organizes objectives into a

mutually exclusive and collectively exhaustive configuration, but also lends itself to the development of evaluation measures for assessing various alternative strategies.

3.4 Development of Evaluation Measures

The identification and organization of the fundamental objectives concerning a given decision problem provide considerable qualitative insight regarding the frame of the decision and possible alternative solutions. However, if alternatives are to be quantitatively analyzed, it is necessary to develop evaluation measures for the achievement of recognized objectives. Keeney points out that,

> measuring the achievement of the fundamental objectives and developing a value model using these objectives can enhance the process and benefits of the value-focused thinking…Specifically, the measurement of objectives clarifies their meaning, and this may lead to the creation of desirable alternatives – perhaps even an obvious 'solution' to a problem. (Keeney, 1992:99)

Evaluation measures are also referred to in the literature as *attributes*, *measures of effectiveness*, *measures of performance*, *criterion*, and *metrics* (Keeney, 1992:100, Kirkwood, 1997:24).

There are four primary types of measures that can be utilized to evaluate the attainment of objectives. Measures can be natural/direct, natural/proxy, constructed/direct, or constructed/proxy. The distinction between these types of measures is discussed below.

3.4.1 Natural vs. Constructed Measures

Natural measures "are those in general use that have a common interpretation to everyone" (Keeney, 1992:101). These measures lend themselves easily to the evaluation of the associated objective. As an example, if the objective is to minimize cost, the evaluation measure "cost measured in dollars" is a natural measure (Keeney, 1992:101). Natural measures are preferred when at all possible, though they are often not available (Kirkwood, 1997:25). In many cases it is necessary to use a constructed measure.

Because there are no existing natural measures for many objectives, constructed measures can be "developed specifically for a given decision context" (Keeney, 1992:102). Examples of objectives with no natural scale include "'improve the image of the corporation' in a business context, 'minimize facial disfigurement' in a medical context, and 'increase the international prestige of the country' in a governmental context" (Keeney, 1992:101). Additionally, at the national level, the security of the homeland involves an array of objectives that may have no clear, universally accepted means of measurement. In cases such as this, constructed measures not only allow for the evaluation of objectives, but also help to define what is meant by the objective (Keeney, 1992:102).

Though the distinction between natural and constructed is explicitly defined, in reality it is often unclear exactly where a given measure falls. In many cases, a measure can be defined as either natural or constructed depending on whom is consulted (Kirkwood, 1997:24).

3.4.2 Direct vs. Proxy Measures

"A *direct* scale directly measures the degree of attainment of an objective, while a *proxy* scale reflects the degree of attainment of its associated objective, but does not directly measure this" (Kirkwood, 1997:24). Direct measures are preferred, as they provide for the evaluation of the exact objective that was intended. In the example of minimizing cost in the previous section, the use of cost in dollars is a direct scale. On the other hand, gross national product represents a proxy scale for the economic well-being of a country (Kirkwood, 1997:24). Thus, proxy measures are used when it is infeasible or impractical to directly measure the attainment of a given objective.

Much like the distinction between natural and constructed, the specification of a measure as direct or proxy can be unclear (Kirkwood, 1997:25). Many measures, such as gross national product, have been in use for such a long time that, in some arenas, they begin to be considered as direct measures of the associated objective (Kirkwood, 1997:25).

The combination of natural or constructed and direct or proxy produces four possible types of measures. Table 3-1 displays the types of measures, labeled in order of decreasing preference with 1 being most preferred (Parnell, 2002).

Table 3-1: Evaluation Measure Preferences

	Natural	Constructed
Direct	1	2
Proxy	3	4

Evaluation measures that are natural-direct are most preferred, because they provide a generally excepted scale for measuring the attainment of the specified objective. Constructed-proxy measures are least preferred because the analyst is forced to develop a metric specifically tailored to evaluating the attainment of a related, rather than specified, objective.

Unfortunately, the most preferred measures are often the most difficult to attain (Chambal, 2002:np). Because the structuring of values is an inherently qualitative process, it can sometimes be all but impossible to identify direct quantitative measures. The analyst is then forced to resort to a proxy scale in order to obtain a natural measure, or in the least preferred case, a constructed measure (Kirkwood, 1997:25). Nevertheless, evaluation measures, regardless of type, supply an indispensable quantitative component to the VFT process.

3.5 Single Dimension Value Functions

The successful identification and specification of objectives, formed into a hierarchical structure, along with evaluation measures for the lowest-level objectives complete the value hierarchy. However, in order to develop a complete, operational value model that can be used to assess and rank various alternatives, it is necessary to generate some method for combining the evaluation measures into a "single index of the overall desirability of an alternative" (Kirkwood, 1997:55). In other words, a method is needed to combine the scores an alternative receives for each measure into a single score. This suggests the development of single dimension value functions (SDVFs).

The chief difficulty in combining scores stems from the fact that different measures can incorporate dissimilar units and varying directions of preference. Whereas one measure may quantify the attainment of an objective in dollars, another measure may assess an objective in terms of hours, or raw numbers, or percentages. Further difficulties in combining measures arise from the use of disparate ranges of measurement. In many cases, changing the range of measurement can affect the ranking of the alternatives (Kirkwood, 1997:58). The final difficulty to be overcome in developing a methodology to combine evaluation measures is the fact that variations over the specified range of the measure cannot always be treated as having equal importance (Kirkwood, 1997:58). As an example, if a measure is defined over the range from 0 to 10, the decision-maker may value an increase from 0 to 5 more than he or she values the increase from 5 to 10. Cases such as this produce nonlinear SDVFs. These and other types of SDVFs are described below.

By creating an SDVF, an alternative can be scored on a 0 to 1 scale for each evaluation measure; 0 being the least value and 1 being the most value. In this way, each alternative is evaluated on the same unitless scale for each measure. As an example, suppose one objective was to maximize the percent of individuals in the United States receiving an inoculation. The range, or x-axis, for this measure would obviously be 0 to 100 percent. Because the objective is to maximize, higher percentages are more preferable. There are a variety of SDVFs that could be developed for this measure.

Suppose the decision-maker decided that every percent increase in inoculations was of equal value. This would produce the linear SDVF shown in Figure 3-2.

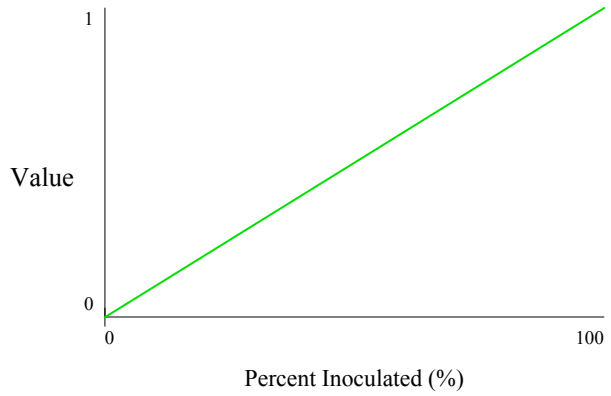

Figure 3-2: Linear SDVF

This function would suggest that an increase from 20% inoculated to 30% inoculated, for example, receives an equivalent increase in value to an increase in inoculations from 70% to 80%. On the other hand, the decision-maker may decide that there is very little value attained until 80% of the population has been inoculated. In this case, the SDVF may take on a more convex appearance, as in the Figure 3-3.

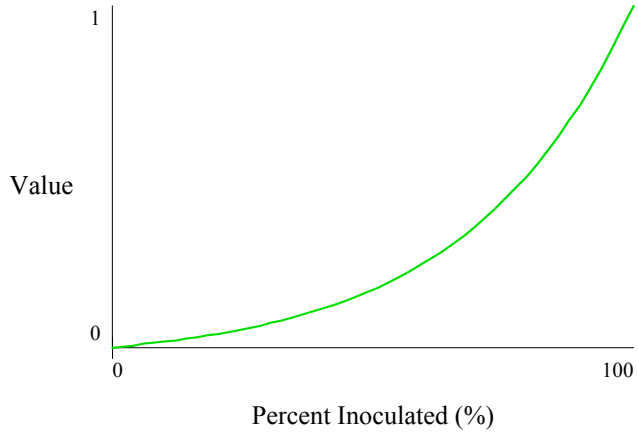

Figure 3-3: Nonlinear SDVF

These two SDVFs are defined on a continuous scale. Linear, piecewise linear, positive exponential, negative exponential, and S-curves are all forms of continuous functions that have been used as SDVFs.

Another approach may be to form discrete "bins" that the scores can fall into. Suppose the decision-maker decided to pursue inoculation of 100% of the population according to the region of the country (time zone) in which they reside. In other words, achieving 100% inoculation in one region would not receive as much value as two, three, or four regions. A discrete SDVF such as this may appear as follows.

# Regions	Value
4 Regions	1.000
3 Regions	0.750
2 Regions	0.500
1 Region	0.250
0 Regions	0.000

Figure 3-4: Discrete SDVF

In the discrete case, only a finite number of values exist for an alternative to receive. If the alternative falls in the least preferred "bin" it receives a 0, whereas if it falls in the most preferred "bin" it receives a 1.

There are a variety of methods available for determining SDVFs. Kirkwood advocates methods for creating exponential functions that incorporate parameters established by the decision-maker (Kirkwood, 1997: 61). Exponential functions such as these are used extensively in Chapter 4 in the development of SDVFs for the homeland

security hierarchy. Regardless of the functional form utilized, the development and implementation of SDVFs are vital to the use of value hierarchies as a means to assess and rank alternatives.

3.6 Summary

The VFT process described above comprises the methodology employed in this thesis. The complex problem facing homeland security decision-makers has been clearly identified. The value trade-offs between security, resource costs, and impact on civil liberties must be addressed if alternative strategies for securing the homeland are to be evaluated. This evaluation is dependent on the capability to clearly identify and organize the objectives associated with homeland security in a manner conducive to measuring the attainment of those objectives. Chapter 4 presents the development of a value hierarchy, along with the associated measures of effectiveness and SDVFs, for assessing alternative homeland security strategies.

4. Homeland Security Strategy Evaluation

4.1 Introduction

As was discussed in the previous chapter, the overall objective of securing the homeland from terrorism involves multiple value trade-offs. At the federal level, the United States government must be concerned with preventing acts of terrorism while at the same time protecting and preparing the nation's citizenry for the possibility that attacks do occur. However, these security efforts are not free. The security of the homeland is a costly endeavor, both fiscally and logistically. More critically, increases in security measures potentially run the risk of infringing on the civil liberties that define the United States as a democratic nation "with liberty and justice for all." These trade-offs must be considered in the evaluation of alternative homeland security strategies.

This study models the complex homeland security decision problem using three distinct value hierarchies; accounting for homeland security, resource costs, and civil liberties. All of these models are used collectively for the same purpose, to select the strategy that has the most favorable impact on the current homeland security posture of the United States. In particular, the homeland security hierarchy facilitates the identification of gaps in the United States government's capability to execute a number of critical objectives and aids in the search for a strategy or set of strategies that close these gaps in the most effective manner.

JP 1-02 defines *strategy* as,

> The art and science of developing and employing instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 1-02, 2001:417)

The instruments of national power include people, plans, policies, procedures, equipment, and actions pertaining to the security of the United States. Thus, for the purposes of this research, a homeland security strategy is defined as any collection of people, plans, policies, procedures, equipment, and actions that are designed to improve the capability of the federal government to achieve the national objectives for homeland security. The hierarchies described in the following sections are designed to evaluate such a strategy or strategies, incorporating subject matter experts' opinions and decision-maker's considered preferences.

4.2 Modeling Homeland Security

The overall objective of the hierarchy described in this section is to capture how well a particular strategy secures the homeland from terrorist threats and acts. The development of this hierarchy requires the identification of what is valued in the homeland security posture of the United States. It is important to note, "homeland security is focused on terrorism in the United States" (National Strategy, 2002: 2). Though terrorism is of worldwide concern, **homeland security** solely addresses terrorist threats to, and acts within, the United States. *The National Strategy for Homeland Security* provides the following definition of homeland security.

> Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy, 2002:2)

This definition establishes the overarching objectives associated with the United States' homeland security posture.

- The prevention of terrorist attacks;
- The reduction of America's vulnerability to terrorism;
- The preparedness to respond to terrorist attacks that do occur.

In order to prevent terrorist attacks, it is necessary "to detect terrorists before they strike, to prevent them and their instruments of terror from entering our country, and to take decisive action to eliminate the threat they pose" (National Strategy, 2002:2). To reduce America's vulnerability to terrorism it is vital that the nation's critical infrastructure and key assets are thoroughly assessed and that every effort is made to protect them (National Strategy, 2002:2). Finally, in order to have the capability to minimize the damage and recover from terrorist attacks, it is necessary "to improve the systems and prepare the individuals that will respond to acts of terror" and to "be prepared to protect and restore institutions needed to sustain economic growth and confidence, rebuild destroyed property, [and] assist victims and their families" (National Strategy, 2002:3). These objectives correspond to the values represented in the first two tiers of the value hierarchy in Figure 4-1. Based on a detailed analysis of homeland security resources, these values were further specified to establish the full hierarchy.

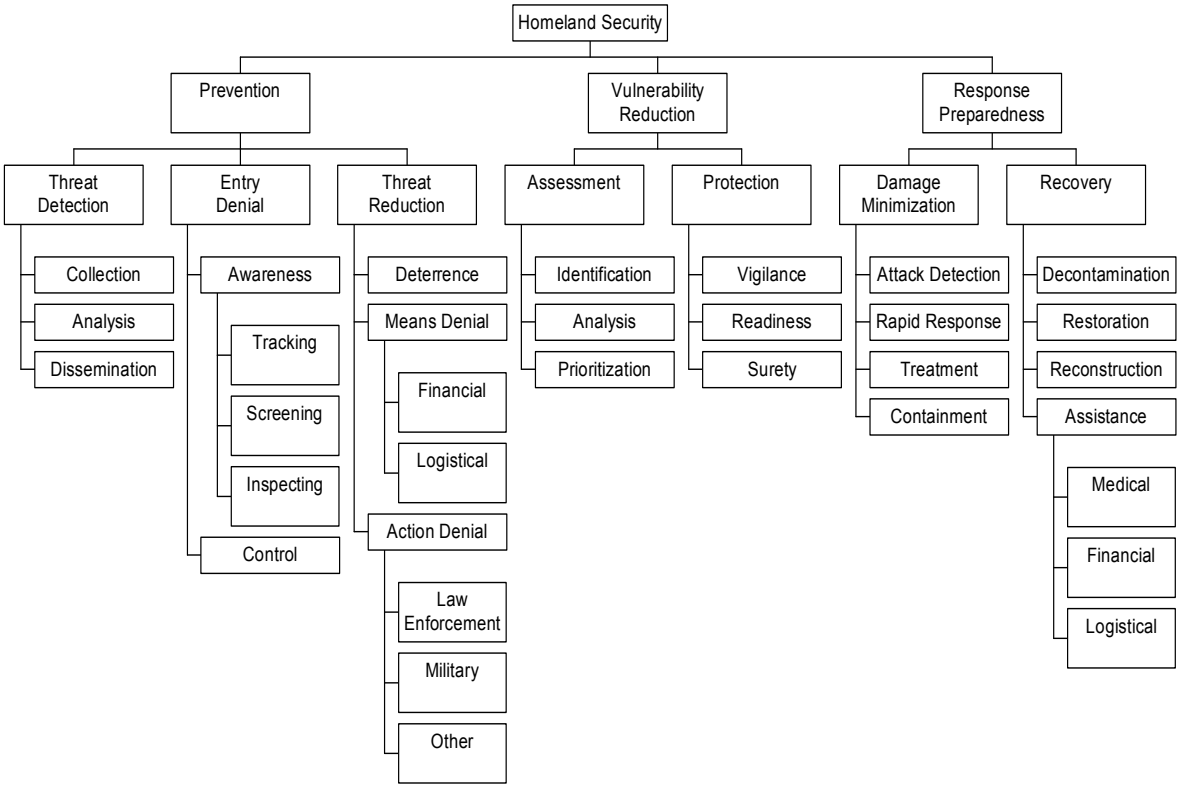

Figure 4-1: Homeland Security Value Hierarchy

As was described in Chapter 3, a value hierarchy should be designed such that it is mutually exclusive and collectively exhaustive. Mutual exclusivity requires that no two objectives stemming from the same parent node overlap. In other words, homeland security efforts should not "double count" a particular element. To be collectively exhaustive, the objectives expressed at each tier of the hierarchy must adequately account for all relevant factors necessary to evaluate the overall objective of securing the homeland. In order to ensure that the value hierarchy is mutually exclusive and collectively exhaustive, each of the three first-tier values is defined in Table 4-1.

Table 4-1: Homeland Security Value Definitions

Homeland Security Value Definitions
Prevention: Actions undertaken to detect terrorists before they strike, to prevent terrorist weapons and those who would use them from entering the United States, and to eliminate the threat they pose. (modified from National Strategy:2) ***Vulnerability Reduction***: Actions undertaken to assess America's critical infrastructure and key assets, and to make every effort to protect them from possible terrorist attacks. (modified from National Strategy:2, 33)
Response Preparedness: Actions undertaken to build and maintain the capability to minimize the damage of and recover from terrorist attacks that occur within the United States. (modified from National Strategy:3)

Detailed definitions for the remaining values in the hierarchy are provided in Appendix C and will not be repeated here. To provide further clarification, each of the three overarching values associated with homeland security is discussed below.

4.2.1 Prevention

Prevention of terrorist attacks within the United States has been acknowledged as the first priority in homeland security (National Strategy, 2002:2). JP 1-02 defines prevention as, "the security procedures undertaken by the public and private sector in order to discourage terrorist acts" (JP 1-02, 2001:344). Discouragement of terrorist acts involves a variety of activities. The prevention of terrorism, as it is categorized in this research, focuses on the threat itself. That is, preventative actions are aimed at known or suspected terrorists, terrorist groups, and their support. In particular, this value applies to the *Intentions* and *Capabilities* portions of the threat model described in Chapter 1. The *Vulnerabilities* portion is discussed in section 4.2.2. Recall that this model states,

Vulnerabilities x Intentions x Capabilities = Threat.

Many of today's terrorists are intent on inflicting as devastating an attack as possible, both in physical and psychological terms. Often, these attacks are specifically designed to inflict harm on non-combatant civilians. To prevent terrorism, it is vital that the individuals with the intent and capability to attack America and her allies are identified and assessed. President Bush noted that,

> Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their activities will improve the government's ability to disrupt and prevent terrorist acts. (Bush, 2002a:14)

In order to **detect** terrorist threats to the United States, it is necessary to first **collect** information pertaining to terrorists and their activities. Once the data is collected, it must be **analyzed** to produce useful intelligence and **disseminated** to the appropriate users.

Moreover, once identified these individuals must be **denied entry** through the United States' land, sea, air, and space borders. The United States must "manage who and what enters [the] homeland in order to prevent the entry of terrorists and their instruments of terror while facilitating the legal flow of people, goods, and services on which our economy depends" (National Strategy, 2002:22). In order to deny access to a given threat, the appropriate agencies must be **aware** of who and what is approaching the nation's borders and have the capability to **control** the entry of people and goods.

Finally, the threat posed by these individuals must be **reduced** by removing the capability and/or intent necessary to carry out attacks. Actions taken to **deter** terrorism address the *Intentions* portion of the threat model, while actions aimed at the means of terrorist attack and the terrorists themselves address the *Capabilities* portion. The United States can **deny the means** of terrorist attack by targeting their **financial** support or by

eliminating their ability to acquire the **logistics** (weapons and delivery systems) necessary to execute an attack. In addition to aiming at the means of attack, the United States can reduce terrorists' capabilities by **denying the actions** of terrorist personnel and their supporters. These actions can be preemptive or retaliatory and can be carried out by **law enforcement**, the **military**, or by **other** authorized agencies or organizations.

The *Prevention* branch of the hierarchy in Figure 4-1 has eight third tier values. Three of these values break down into a fourth tier of values. The eight fourth tier values, along with the remaining five third tier values, specify *thirteen* national level capabilities that the United States must pursue in order to prevent terrorism. This national level effort to secure the homeland, by focusing on the intentions and capabilities of potential or recognized threats, must be complemented by vulnerability-focused actions aimed at reducing national weaknesses that terrorists might seek to exploit.

4.2.2 Vulnerability Reduction

The *National Strategy for Homeland Security* repeatedly emphasizes the importance of addressing America's vulnerability to terrorism.

> Currently the U.S. government does not perform comprehensive vulnerability assessments of all our Nation's critical infrastructure and key assets. Such vulnerability assessments are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given facility or sector, and then to invest accordingly in protecting such facilities and sectors. (National Strategy, 2002:18)

The reduction of America's vulnerability to terrorism, in this research, focuses on weaknesses internal to the United States. That is, vulnerability reduction is aimed at people, systems, symbols, facilities, functions, and events within the United States. In

particular, this value applies to the *Vulnerabilities* portion of the terrorist threat model discussed in Section 4.2.1. The critical infrastructure vulnerability reduction suggested by the PCCIP, and mandated by PDD 63, is a vital step in the effort to secure the United States from terrorism. Thus, vulnerability reduction, as it is defined here, only addresses the weaknesses of the nation that are associated with the threat of terrorism.

> **Assessing** these weaknesses is a daunting task.
>
> Our open and technologically complex society presents an almost infinite array of potential targets, and our critical infrastructure changes as rapidly as the marketplace. It is impossible to protect completely all targets, all the time. On the other hand, we can help deter or deflect attacks, or mitigate their effects, by making strategic improvements in protection and security. Thus, while we cannot assume we will prevent all terrorist attacks, we can substantially reduce America's vulnerability, particularly to the most damaging attacks. (National Strategy, 2002:29)

Because it is fiscally, logistically, and operationally infeasible to reduce *all* potential vulnerabilities, it is necessary to **identify** who and what is critical to the security, governance, public health and safety, economy, and morale of the nation. The efforts of the PCCIP, and other government agencies, constitute major strides toward accomplishing this identification. Once identified, these critical infrastructure sectors and key assets must be **analyzed** in order to evaluate the consequences of an attack and appropriately **prioritize** protection efforts. This analysis will be dependent, in part, on integrating terrorist threat capabilities and intent with identified weaknesses to establish precedence for protection.

Once the nation's critical infrastructures and key assets have been prioritized according to their associated vulnerabilities, efforts must be made to **protect** them from attack. Protective actions include pre-attack warnings to increase the alertness of

potential targets, the establishment of contingency plans and procedures to prepare the appropriate sectors for addressing the consequences of an attack, and physical and cyber defense measures to secure potential targets from damage. Collectively, these efforts will enhance the **vigilance**, **readiness**, and **surety** of the nation's vulnerable critical infrastructure and key assets.

The objectives associated with the *six* third tier values in the *Vulnerability Reduction* branch specify capabilities that the United States must pursue, at the national level, in order to reduce the vulnerability to terrorism (See Figure 4-1). In addition to the aforementioned objectives of preventing terrorist attacks and reducing America's vulnerability to such attacks, the nation must prepare for the possibility that an attack does occur.

4.2.3 Response Preparedness

No matter how valiant the effort, it is virtually impossible to stop every terrorist or eliminate every potential vulnerability. Accordingly, the nation must be prepared to manage the consequences of an attack.

> Past experience has shown that preparedness efforts are key to providing an effective response to major terrorist incidents and natural disasters. Therefore, we need a comprehensive national system to bring together and command all necessary response assets quickly and effectively. We must equip, train, and exercise many different response units to mobilize for any emergency without warning. (National Strategy, 2002:41)

The nation's preparedness to respond to acts of terrorism, as it is characterized in this research, focuses on activities performed during and after an attack has occurred. Response preparedness is aimed at the planning, training, equipment, and exercises

necessary to prepare the personnel and systems responsible for responding to terrorist attacks within the United States and facilitating recovery from such attacks. The previous two values associated with securing the homeland focused on activities prior to the actual occurrence of an attack. The *Response Preparedness* value addresses the activities necessary to prepare for managing the consequences of an attack that does occur.

Consequence management includes the immediate need to **minimize the damage** of a terrorist incident by **detecting** the occurrence of an attack, **responding rapidly**, providing medical **treatment** to those affected, and **containing** the damage (National Strategy, 2002:38). If an attack is not correctly identified and recognized, then the appropriate response cannot be developed and deployed. Additionally, treating victims to save life and limb and preventing the spread of the attack are paramount to minimizing the damage associated with a terrorist incident. Because the majority of this responsibility is in the hands of America's emergency first-responders, they must be prepared to react to an array of possibilities. The intent here is to capture federal capabilities that support these state and local efforts.

In addition to the immediate response to an attack, it is vital that the United States prepare to **recover** from attacks over a long period of time. This recovery starts with the reconstitution of vital systems, services, and facilities by **decontaminating** the site of the attack as necessary and **restoring** critical infrastructure. The eventual **reconstruction** of the systems, services, and facilities affected by the attack is also of considerable concern. While many of these concerns are local, federal support may be required. Finally, it is important that the federal government have the capability to **assist** state and local

governments in aiding victims and their families with **medical**, **financial**, and **logistical** needs.

The *Response Preparedness* branch of the hierarchy in Figure 4-1 has eight third tier values. One of these values breaks down into three fourth tier values. These fourth tier values, along with the remaining seven third tier values, specify *ten* national level capabilities that the United States must pursue in order to prepare to respond to acts of terrorism.

The combination of the three objectives of homeland security specified in the *National Strategy for Homeland Security*, 1) Prevent terrorist attacks, 2) Reduce America's vulnerability to terrorism, and 3) Prepare to respond to attacks that do occur, embody all that is valued in the homeland security posture of the United States at the federal level. Thus, the clearly defined values *Prevention*, *Vulnerability Reduction*, and *Response Preparedness*, along with the specified underlying values, provide a collectively exhaustive and mutually exclusive hierarchical structure. This structure can be utilized to assess the impact that alternative homeland security strategies have on the Federal government's capability to execute the *29* final tier objectives. Again, detailed definitions of each of the values contained in the hierarchy can be found in Appendix C.

4.3 Measuring the Security of the Homeland

Newly developed strategies to enhance security should target the improvement of the 29 critical capabilities delineated in the value hierarchy in Figure 4-1. In order to measure the impact that a particular strategy has on each of these capabilities, proper

clarification must be given to determine what type of improvements are desired. Strategies aimed at improving the capability to collect information about potential terrorists may simply target greater *quantities* of data. On the other hand, a strategy that seeks to improve the capability to detect biological attacks may have *speed* as its chief concern. These growth areas must be properly clarified for each critical capability in order to define a target level for each of the 29 objectives of interest.

The target capability will be specific to each individual objective and must be clearly defined at the appropriate level of authority. Accordingly, homeland security decision-makers and subject matter experts must clarify a desired, attainable level of capability for each of the 29 objectives. Just as with characterizing the capability itself, in defining the target for each capability, consideration must be given to a variety of impacts. These include enhancements in speed, accuracy, and effectiveness. Once defined, the target capability represents the desired or "100%" level of capability. The costs, in money, time, and manpower, associated with attaining the desired capability level are considered in Section 4.4.

The minimum acceptable level of capability must also be defined. For each of the 29 objectives, the same homeland security decision-makers and subject matter experts must clarify the lowest level of capability that the United States would be willing to accept. This lower bound or "0%" level of capability, along with the upper bound provided by an achievable target capability, produces the continuum displayed in Figure 4-2.

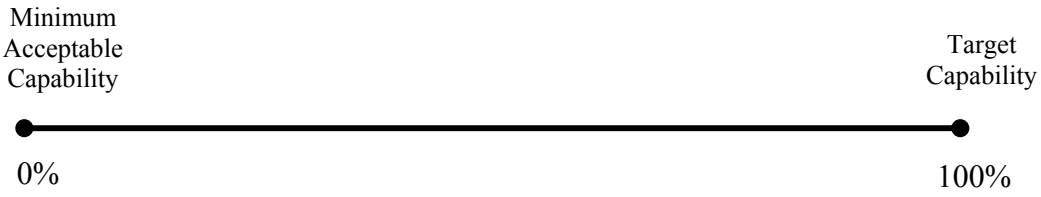

Figure 4-2: Capability Continuum

It will be a major task to establish the desired minimum requirements and desired target levels for this continuum. Clearly, in an ideal world, full security against any known or unknown type of threat or attack would be the 100% target level. For practical purposed this is not an attainable goal, even in a static environment, let alone in the dynamic world in which we live. People of reason and good intent will be needed to determine these minimum thresholds and desired target capabilities. Current *and* forecasted threats will need to be considered in conjunction with current *and* forecasted technological capabilities to establish a practical time horizon. Finally, targeted goals will likely need to be dynamic to adjust to adaptable foes. Though exact capability continuums for each of the objectives in the value hierarchy cannot be constructed in this research, without the support of Federal level homeland security decision-makers, Appendix D delineates the issues that would likely be considered in this process. Once completely and clearly established, the capability continuums can be utilized to assess the United States' current capability to accomplish each of the 29 objectives in the homeland security value hierarchy.

Using the minimum acceptable and target capabilities as a basis for comparison, the current capability must be identified on the capability continuum. The current capability is defined by determining what percent of the target capability the Federal

government currently achieves. This definition can only be established after careful consideration has been given to all of the potential impacts described in the determination of the target capability (i.e. speed, accuracy, and so forth). The percent is then annotated on the capability continuum. If the relevant decision-makers and subject matter experts ascertain that the current capability is equal to or falls below what has been defined as the minimum acceptable level, then the current capability is defined as 0%. Similarly, if it is determined that the current capability is equal to or exceeds the target capability, then the current capability is defined as 100%.

The gap between the current capability and the target represents the desired improvement that a new homeland security strategy could assist in providing. In other words, if the current capability is defined as x%, then the Federal government has a capability gap of (100 – x)% that needs to be reduced by alternative homeland security strategies. Figure 4-3 displays this capability gap.

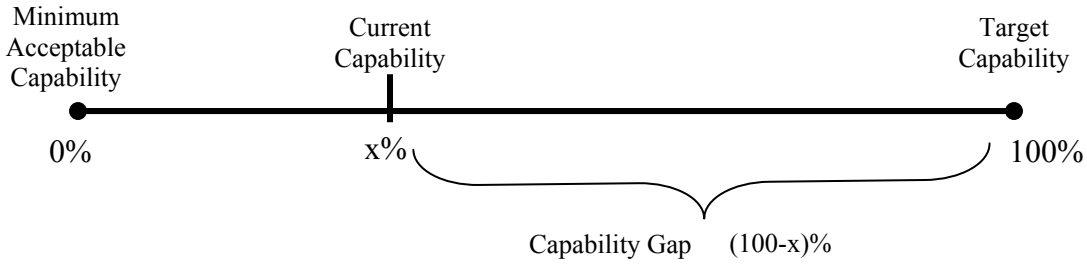

Figure 4-3: Capability Continuum with Gap

Ideally a strategy, or set of strategies, would completely close this gap, thus providing full capability to execute the associated objective. Unfortunately, this can be difficult and costly. If the current capability is determined to be relatively low, it may

require a significant amount of resources to completely close the large gap in capability. Regardless, the Federal government needs to close these capability gaps as much as possible. Accordingly, *this research measures the impact that a proposed strategy has on the United States' capability to execute homeland security objectives by assessing the percent closure in the associated capability gap*. If a particular strategy fails to close the gap at all on a specific measure, or actually increases it, then it will receive the minimum value of zero for that measure. On the other hand, if a strategy facilitates a complete closure in the capability gap of a measure, then it will receive the maximum value of one for that measure. Finally, the value provided by an intermediate percent closure will be dependent on the current capability associated with each objective. These concepts are illustrated in more detail in the following section.

4.3.1 Capability Continuum Development

Early in Section 4.3. the examples of collecting data on potential terrorists and detecting biological attacks were briefly discussed. These two critical capabilities are leveraged in this section in the development of an illustrative example.

Suppose the appropriate decision-makers and subject matter experts were assembled and tasked with constructing measures that could be utilized to assess the impact that new technological innovations would have on the Federal government's capability to collect information about terrorists and to detect biological attacks. To accomplish this, the panel of experts will be required to define desired minimum requirements, desired attainable target capabilities, and the current capability.

For data collection, the experts might develop a comprehensive list of information (including identification, financial, travel, association, and background data) that they feel will be required to track down terrorists. In defining the target capability to obtain this data, the panel might consider the quantity that is accessible, the speed with which it can be acquired, and the accuracy of the data as it is applicable to developing useful intelligence. These same issues would be under consideration in the establishment of a minimum acceptable capability to collect data. Once the bounds were clearly defined, the experts would be required to assess the Federal government's current capability to collect vital information about terrorists.

For the purposes of this example, suppose the current capability was determined to be 90% of the way between the minimum and target capability. The capability continuum in Figure 4-4 displays this assessment.

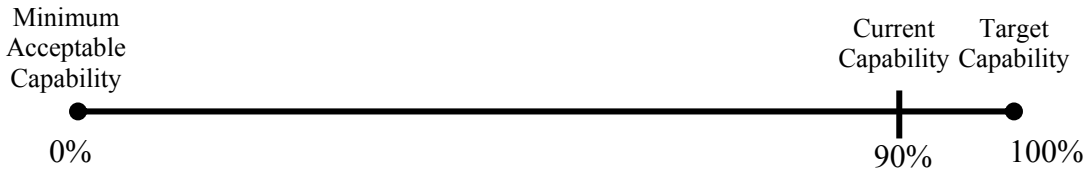

Figure 4-4: Data Collection Capability Continuum

The assessment of a current capability of 90% defines a capability gap of 10%. Thus, there is limited room for improvement to this capability. This suggests that the decision-makers would value the closure of a small gap marginally less than a large gap in capability, all other things being equal. If this is not the case, the weighting of the

hierarchy will capture these differences in preference between objectives. The example of detecting biological attacks provides a contrast to this assessment.

For detecting biological attacks within the United States, the panel of subject matter experts might determine that the attack must be identified and recognized within a certain period of time in order to affect a response. Thus, the speed of detection, as well as the accuracy of recognition, would be vital factors in defining the target capability. Ideally, the attack would be quickly identified and accurately recognized in a timely enough manner to facilitate the complete containment of the effects. On the other hand, experts would need to define a minimum detection capability that allowed for the lowest acceptable scale of response. Just as with the previous example, once these bounds were defined the current capability would be determined. In this example, the current capability is defined as 10% of the target level. Figure 4-5 depicts the capability continuum for this measure.

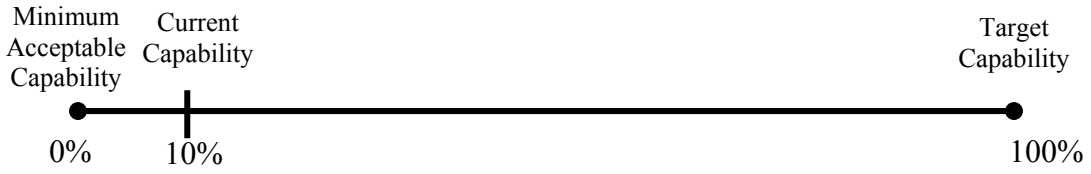

Figure 4-5: Attack Detection Capability Continuum

With a current capability of 10%, the objective of detecting biological attacks has a large capability gap of 90%. In this case, new strategies aimed at improving the nation's capability to detect biological attacks could provide significant improvement. This suggests that decision-makers would assign a large value to even a small percent closure

in the capability gap. It follows that *the value assigned a percent closure in the capability gap is dependent on the size of the gap itself*; i.e. the magnitude of the targeted capability shortfall.

In this illustrative example, the current capability to collect information about potential terrorists was identified as 90%. Suppose a proposed strategy provided a 50% closure in the 10% capability gap for this objective. The current capability would only be increased to 95%. While valued, the impact of a 5% increase in capability is a small marginal increase. Figure 4-6 demonstrates the improvement provided by this strategy.

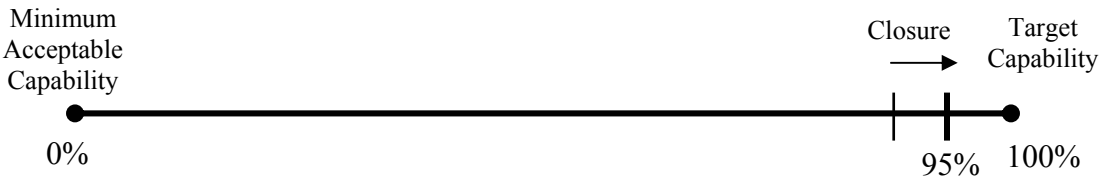

Figure 4-6: Data Collection Improvement

In contrast, a 50% closure in the capability gap associated with the detection of biological attacks would provide a dramatic increase in capability. In this example, the current capability to detect biological attacks was defined as 10% on the continuum. The same 50% closure, in this case, would increase the current capability to 55%. All other things being equal, such a closure in the capability gap (see Figure 4-7) would be of high value to the decision-making panel.

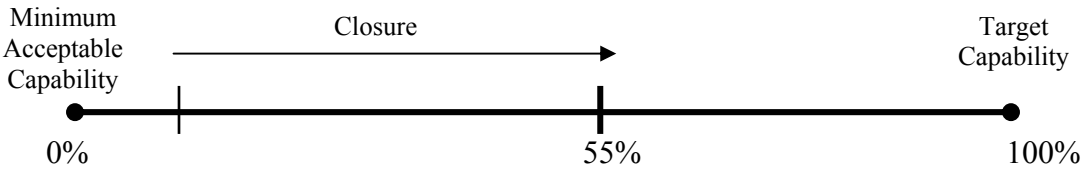

Figure 4-7: Attack Detection Improvement

Thus, some method of measurement (i.e. SDVFs) is needed to model the fact that the value assigned a percent closure in the capability to execute various objectives is dependent on the current capability as determined by subject matter experts. If the current capability to execute an objective is relatively low, then even small closures in the capability gap provide high value. However, these returns in value diminish as the percent closure approaches 100. Alternatively, if current capability were high, then even moderate closures would provide very little additional value. In this case, the returns in value increase as the percent closure approaches 100. This need to acquire a value function that relies on current capability as a parameter suggests the development of exponential SDVFs similar to those described by Kirkwood (Kirkwood, 1997:64-65). By using these functions, decision-makers can account for the value achieved by strategies that close the capability gaps associated with objectives that have varying current capabilities. Recall, however, that the hierarchy will be weighted to reflect the relative importance of each measure. It is possible that the closure of a 10% capability gap for one measure is more important than the closure of a 90% gap for another measure, if the measure receives a very high weight. The exponential functions, and their application to the ongoing example in this section, are described in Section 4.3.2.

4.3.2 Exponential SDVF Development

Exponential SDVFs were considered the most appropriate value functions for the measurement of the objectives in the security hierarchy. They allow for the use of current capability as a parameter, and they model the diminishing/increasing returns in

value associated with dissimilar percent closures in the capability gap. The example of the previous section is again utilized here to provide a general illustration of such functions, followed by the exact formulation.

The notional, current capability of the Federal government to collect vital information about terrorists has been defined by subject matter experts, in this example, to be 90% on the continuum. Because of this, decision-makers would value minor closures in the 10% capability gap less. On the other hand, as the percent closure approaches 100%, the value is assumed to increase. The function in Figure 4-8 demonstrates this behavior.

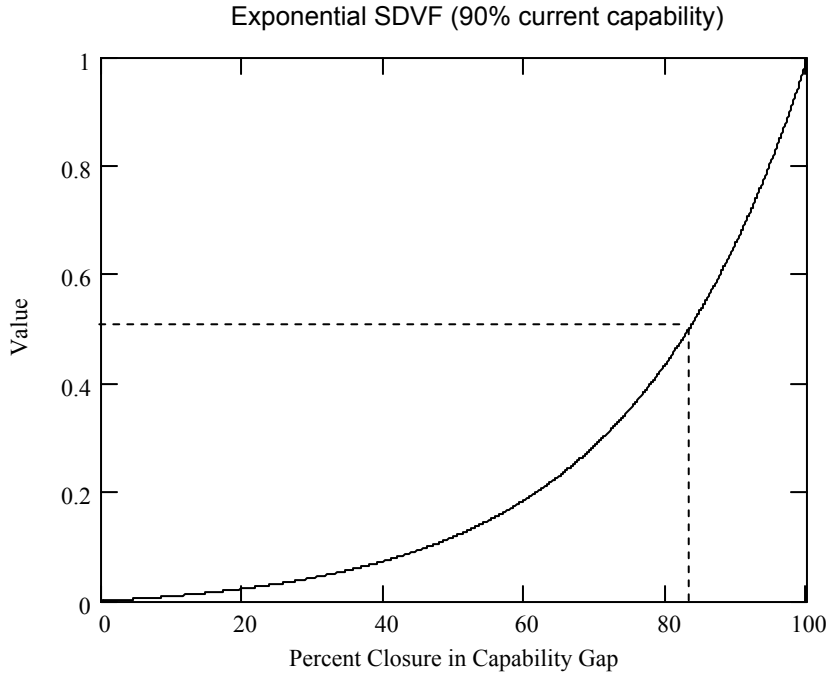

Figure 4-8: Exponential SDVF (90% current capability)

As desired, very little value is achieved until the capability gap is closed dramatically. In fact, a new strategy would not even receive half of the possible value, in this case, until the gap was closed by over 80% (see Figure 4-8). This follows, because if the current

capability were already 90% it is doubtful that decision-makers would wish to invest in a strategy unless it would nearly provide them with "full" capability, all other things being equal. The example of detecting biological attacks provides a contrast to this case.

In the example used in this research, the current capability of the Federal government to detect biological attacks is notionally defined as 10% on the capability continuum. In this case, even minor closures in the 90% capability gap are assumed to provide high value to the relevant decision-makers. This percent closure would demonstrate diminishing returns in value, however, as it approached 100%. Figure 4-9 depicts the function used in this case.

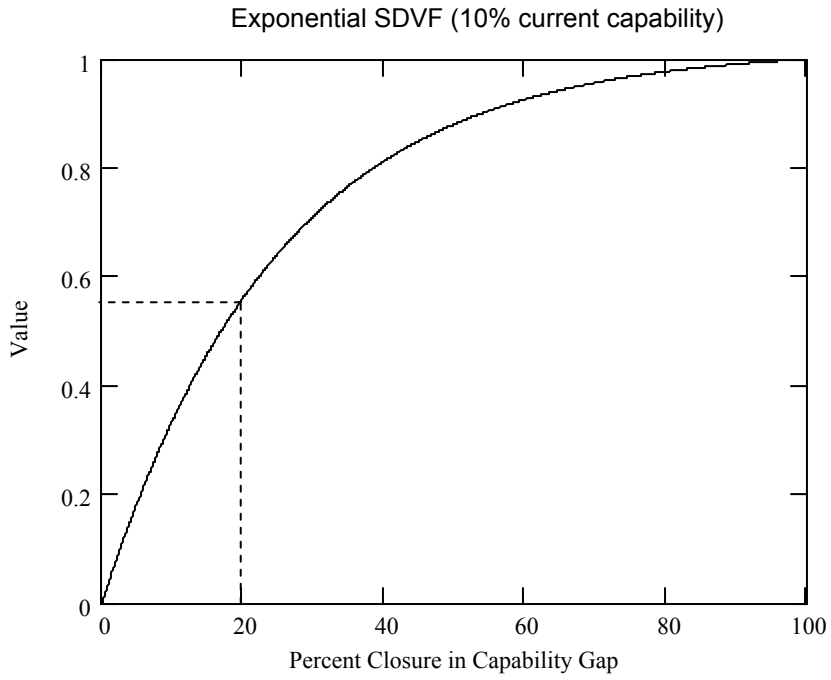

Figure 4-9: Exponential SDVF (10% current capability)

With a low current capability (i.e. 10%) a great deal of value is achieved by even a small percent closure in the capability gap for a specific measure. A proposed strategy would

receive more than half of the possible value for a 20% closure in the large gap in capability (see Figure 4-9). With such a small existing capability in this critical area, homeland security decision-makers would likely be willing to invest in a strategy that provided even a little closure, all other things being equal. Thus, the value function displayed in Figure 4-9 makes logical sense. The remainder of Section 4.3.2. delineates the exact formulation of these functions.

The driving factor in this section has been that the value assigned to improvements in the critical capabilities defined earlier in this chapter is dependent on the current capability in that area. It is only logical then that current capability would be a parameter in the calculation of value. Given the definition of current capability, the value function used to measure improvements (i.e. closures in the capability gap) in the Federal government's capability to execute homeland security objectives follows.

Let C_i = current capability (as a percent defined on the continuum) to execute the objective associated with measure *i*. The SDVF for measure *i* would be as follows.

$$V_i(x) = \begin{cases} 1, & \text{for } C_i = 100 \\ \dfrac{x}{100}, & \text{for } C_i = 50 \\ \dfrac{1 - e^{-x \cdot R}}{1 - e^{-100 \cdot R}}, & \text{otherwise} \end{cases}$$

where $$R = \frac{50 - C_i}{\rho}, \quad \text{for } \rho > 0.$$

The parameter ρ accounts for the value preferences of the decision-makers being solicited to create the SDVFs. A detailed discussion of these preferences will not be given here;

however, it is important that the value functions used in this research allow for the possibility of differing opinions regarding the shapes of the curves. In general, the smaller ρ becomes, the more drastic the curves become as the current capability moves away from 50%. In this research, ρ is defined as **1000**.

Once ρ has been defined, and the current capability (C_i) is established, the value for R can be entered into the equation $V_i(x)$. For measure i, $V_i(x)$ defines the value achieved by an x % closure in the gap between the current capability C_i and the target capability. The graph depicted in Figure 4-10 displays the SDVFs given current capability equal to 0, 10, 20, 30, 40, 50, 60, 70, 80, and 90 percent of the target level. These current capabilities are annotated on each of the curves.

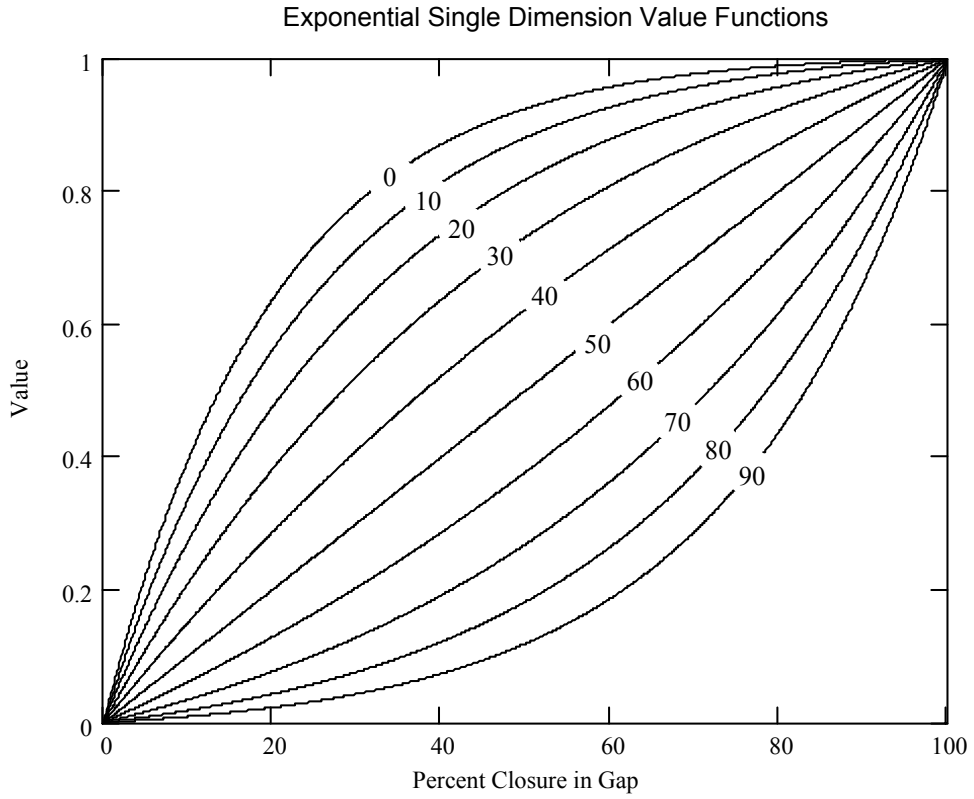

Figure 4-10: Exponential SDVFs

As desired, when current capabilities are low, even minor closures in the capability gap provide significant value. As the current capability decreases from 50%, the curves display increasingly diminishing returns in value. Similarly, when current capabilities are high, the gap must be closed considerably to attain even a little value. As the current capability increases from 50%, the curves display increasingly enhanced returns in value. In the case that current capability in defined as exactly 50% of the desired level, the return in value is linear.

It should be noted that if the current capability for a particular objective were 100% of the target level, then no gap would exist and every alternative that fails to decrease capability would automatically score a value of 1 for that objective. This does not suggest that a strategy to address this capability is senseless. Decision-makers may deem it necessary to pursue a strategy that increases capability beyond the target level. However, in this research, such strategies will not achieve more than a value of 1. This suggests, however, periodic reviews of the target capabilities. They may be re-set as capabilities and technologies change.

One potential concern that has yet to be addressed is the possibility of dissimilar assignments of importance among the 29 critical objectives defined in the value hierarchy in Figure 4-1. It could be argued, for example, that investments should be made to provide minor closures in the data collection capability gap, even though a high level of capability already exists. Perhaps the mission is *so* critical that the value assigned by the SDVF does not completely capture the decision-maker's intent. Issues such as these would be accounted for by **weighting** the value hierarchy. By weighting the measures and values included in the hierarchy, decision-makers can account for their preferences

and assign dissimilar levels of importance. The value hierarchy will not be weighted in this thesis. Such weighting, though critical to the complete application of the value model, is dependent on the expertise provided by homeland security decision-makers, and is therefore beyond the scope of this research. In addition, the actual weights (priorities) of national objectives would likely be deemed classified. Regardless, Appendix A does provide a description of the weighting process.

4.3.3 Summary for Security Measures

For each of the 29 critical objectives defined in Sections 4.2.1-4.2.3. the exponential SDVFs described in this section provide a means to measure the impact that new homeland security strategies have on federal level capabilities. The identification of minimum acceptable and target capabilities for each objective is vital to the application of these measures. The subsequent assertion of current capabilities in each area defines capability gaps that the United States must make every effort to close. However, it is vital that the appropriate decision-makers and subject matter experts properly clarify minimum, target and current capabilities. Without their expertise, the capability gap cannot be accurately assessed. While beyond the scope of this effort, it clearly is a necessary step to take in order to secure the homeland. As previously stated, to assist this clarification, Appendix D describes issues that might be considered in the development of a capability continuum for each of the 29 objectives. Finally, the data gained from the assessment of minimum, target, and current capabilities must be applied to the

development of value functions that accurately model the decision-maker's preferences. The exponential SDVFs presented in this section accomplish this goal.

4.4 Consideration of Resource Costs

"The national effort to enhance homeland security will yield tremendous benefits and entail substantial financial and other costs" (National Strategy, 2002:63). Accordingly, a complete analysis of the homeland security posture of the United States must consider the costs associated with attaining the desired level of security. By definition, the effort to secure the homeland from terrorism is a responsibility shared by the federal government, state and local governments, the private sector, and the American people (National Strategy, 2002:2). Consistent with the scope of this research, the cost hierarchy described in this section addresses the key role played by the federal government in allocating resources to homeland security. However, because reduced spending at the federal level can potentially lead to increased cost at the state and local levels, the allocation of resources at all stages of government are considered in this hierarchy. Additionally, increases in security have the potential to negatively impact the United States economy as a whole or in particular sectors of the economy. This suggests that decision-makers should balance where they spend their money, as well as the economic impact that the purchased security measures incur. The resource allocation considered in this research certainly includes monetary aspects; however, the time and personnel required to carry out proposed security strategies must also be considered. Figure 4-11 illustrates the cost hierarchy utilized in this research.

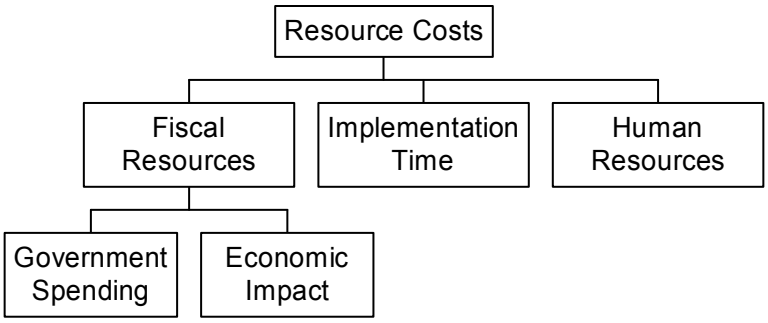

Figure 4-11: Resource Costs Hierarchy

For this thesis, *Fiscal Resources* accounts for the portion of federal, state, and local budgets that is allocated to implementing a proposed homeland security strategy as well as the economic impact of that implementation. *Implementation Time* accounts for the amount of time necessary to completely implement all portions of the planned strategy. Finally, *Human Resources* accounts for the acquisition of personnel required at the federal, state, and local level. These three costs are further clarified in the following sections.

4.4.1 Fiscal Resources

It is vital that any proposed strategy to secure the homeland recognizes the economic cost associated with implementation. The Bush Administration "intends to provide whatever resources are necessary to secure the homeland, but is committed to ensuring that the taxpayers' money is well spent" (Bush, 2002b:8). In order to ensure the proper distribution of federal, state, and local dollars, it is necessary to "carefully weigh the benefit of each homeland security endeavor and only allocate resources where the benefit of reducing risk is worth the amount of additional cost" (National Strategy,

2002:64). Since 9/11 homeland security activities have received a drastic increase in funding. Figure 4-12 depicts the portion of the federal budget, including Emergency Relief Funds (ERF), which has been allotted to homeland security activities since FY 1995. It should be noted that the Bush Administration estimated the figures for FY 1995 through FY 1997, as the Office of Management and Budget (OMB) did not collect this data until FY 1998 (Bush, 2002b:8). A portion of these federal funds have been allocated to assisting state and local governments, however these numbers do not account for the homeland security costs directly apportioned from state and local budgets.

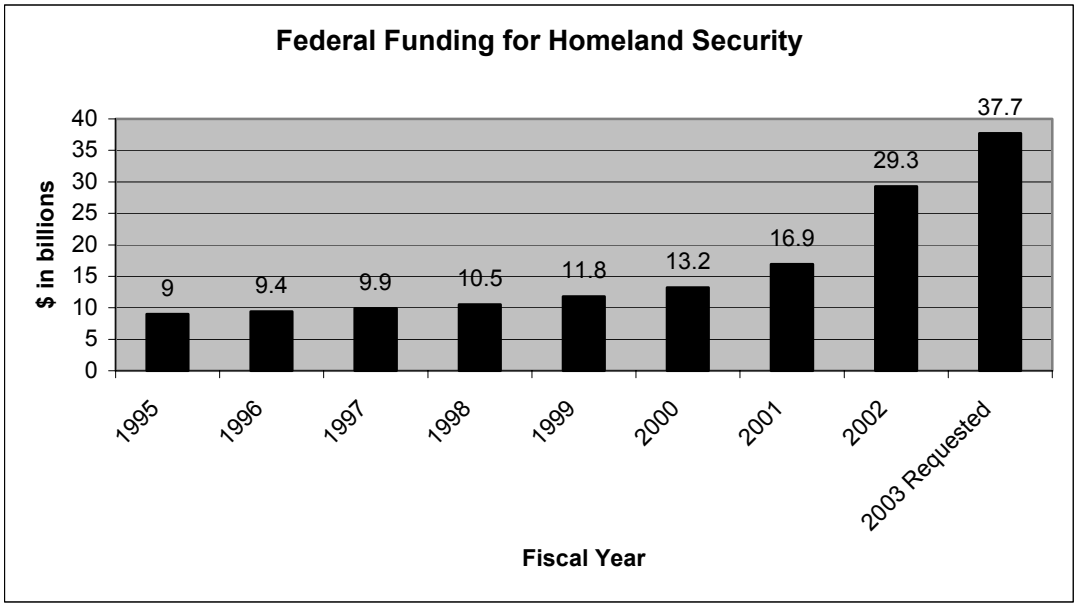

Figure 4-12: Federal Homeland Security Spending

(Bush, 2002b:8)

According to research performed by Deloitte Consulting and *Aviation Week*, state and local governments are projected to spend as much as $5.1 and $13.9 billion respectively in Fiscal Year 2003 (Deloitte Consulting, 2002:1). This projection of homeland security fiscal resource allocation is above and beyond any monetary

assistance from the Federal government. All told, it is projected that all levels of the United States government combined could spend nearly $60 billion on homeland security activities in FY2003.

It is assumed that lower dollar costs are preferred at all levels of government. A strategy that provides a high level of security, but costs nothing would achieve the highest value. However, greater security will ordinarily incur greater costs. The higher the cost of a strategy, the less value it achieves. Thus it is necessary to carefully weigh increases in security against the federal, state, and local budgetary allocation that these increases require. Accordingly, in this research, government spending is measured at all three levels of government.

In addition to reducing spending, homeland security decision-makers should consider the potential negative impacts that enhancements in security might pose for the U.S. economy. The recent hardships experienced by the airline industry, for example, can be attributed not only to the fear instilled on 9/11, but also to newly imposed time requirements that cause passengers drastic delays. These delays are due to added measures to improve security. Every effort should be made to design security measures to avoid unnecessarily hindering American commerce. The development of strategy should balance this consideration along with need to enhance security.

4.4.2 Implementation Time

The urgency of the terrorist threat to the American homeland suggests that an effective security strategy that can be implemented quickly is preferred. However, much like the allocation of fiscal resources, it may prove necessary to allot more time for implementation in order to ensure a higher level of security. For instance, the creation of the Department of Homeland Security may greatly increase the United States' capability to secure the nation from terrorism; however, it could take years to fully organize (Daalder, 2002:iv). This does not necessarily imply that a long-term strategy is an ineffective one; it simply demonstrates how time is a factor that must be considered. In fact, a short-term, poorly planned strategy could cause future problems that far outweigh the benefit of an immediate solution. Nevertheless, in general, the longer it takes to implement a particular strategy, the longer the United States remains unsecured. Thus, it is assumed that a lower implementation time is preferred.

4.4.3 Human Resources

The Department of Homeland Security is merging 22 government agencies with critical homeland security missions and will consist of more than 170,000 personnel (National Strategy, 2002:13, Daalder, 2002:9). Once fully operational, the new Department will be "the third largest federal department in personnel terms" (Daalder, 2002:11). As one strategy for securing the homeland, the creation of the Department of Homeland Security demonstrates the importance of the personnel element. The acquisition or relocation of personnel to execute a particular strategy incurs various costs, as does the training and management of said personnel. It is assumed that the preference

is to minimize the increase in the homeland security workforce, at the federal, state, and local levels, required to implement a proposed strategy. However, like the previous costs, this increase must be balanced in the overall consideration of the homeland security posture of the United States. Table 4-2 summarizes the measures developed for the *Resource Costs* considerations. A more detailed description of each of these measures, as well as their SDVFs, is provided in Appendix E.

Table 4-2: Resource Costs Measures

TITLE	MEASURE UNIT	MEASURE TYPE	LOWER BOUND	UPPER BOUND
Government Spending				
Federal spending	Total cost incurred in NPV	Billions of dollars per strategy (Linear)	0	1
State spending	Total cost incurred in NPV	Millions of dollars per strategy (Linear)	0	140
Local spending	Total cost incurred in NPV	Millions of dollars per strategy (Linear)	0	370
Economic Impact				
Impact on Economy	Potential impact of the strategy on the U.S. economy	Categorical	No Impact	Severe Impact
Implementation Time				
Strategy Implementation Time	Years required to implement all portions of the proposed strategy	Years (S-curve)	0	20
Human Resources				
Federal workforce	Percentage change in workforce required	Percentage (Linear)	0	100
State workforce	Percentage change in workforce required	Percentage (Linear)	0	100
Local workforce	Percentage change in workforce required	Percentage (Linear)	0	100

4.5 Consideration of Civil Liberties

The *National Strategy for Homeland Security* notes the importance of civil liberties.

> Liberty and freedom are fundamental to our way of life. Freedom of expression, freedom of religion, freedom of movement, property rights, freedom from unlawful discrimination – these are all rights we are guaranteed as Americans, and rights we will fight to protect. Many have fought and died in order to establish and protect these rights; we will not relinquish them. (National Strategy, 2002:8)

Though these freedoms are essential to the American way of life, they may potentially be infringed upon by efforts to secure the homeland from terrorism. It is therefore necessary to recognize and consider how a particular homeland security strategy impacts the civil liberties of America's citizenry, as well as those accused of terrorist activity. A newly proposed plan to secure the United States, for example, may dramatically increase the capability of the federal government to combat terrorism; however, this enhancement may be unacceptable due to its infringement on the fundamental freedoms that are the right of all Americans. Wisconsin Democratic Senator Russ Feingold, in a speech to the Senate on 11 October 2001, stated:

> There is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country where police were allowed to search your home at any time for any reason; if we lived in a country where the government is entitled to open your mail, eavesdrop on your phone conversations, or intercept your e-mail communications; if we lived in a country where people could be held in jail indefinitely based on what they write or think, or based on mere suspicion that they are up to no good, the government would probably discover more terrorists or would-be terrorists! But that wouldn't be a country in which we would want to live. (Martin, 2003:2)

Senator Feingold points out three primary freedoms that security efforts may impact; privacy rights, freedom from discrimination, and judicial rights. Unwarranted searches

and intrusions into the personal affairs of innocent Americans would severely infringe on the right to privacy. The discrimination of individuals based on their beliefs or background is another potential negative impact of increased security. Finally, the judicial rights promised to individuals suspected of terrorism should not be neglected. Indefinite detentions, or suspension of habeus corpus are only two ways in which these rights could be neglected. The hierarchy in Figure 4-13 attempts to account for the potential impacts that security efforts may have on civil liberties.

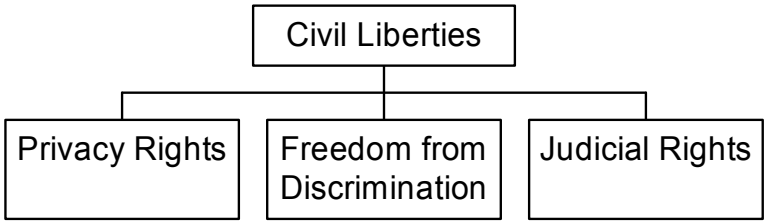

Figure 4-13: Civil Liberties Hierarchy

Each of these values is further clarified in the sections below.

4.5.1 Privacy Rights

The collection and analysis of information pertaining to possible terrorist threats is a vital component to the federal government's effort to secure the United States homeland. However, these activities are potentially in conflict with the privacy rights of America's citizenry. The increased public use of video and other forms of surveillance, the proposed creation of a National ID card, and increased government access to personal, financial, and communication records are a sampling of topics that have raised concern for individual privacy rights. Sections 201 through 225 of the USA PATRIOT

Act, for example, address a variety of enhanced surveillance procedures including the authority to intercept wire, oral, and electronic communications relating to terrorism (107th Congress, 2001:np).

Each year, Privacy International and the Electronic Privacy Information Center (EPIC) perform the Privacy and Human Rights survey to review the state of privacy in over fifty countries worldwide (EPIC, 2002). In its analysis of the United States, the report noted that there is no explicit right to privacy contained within the U.S. Constitution (EPIC, 2002:382). However, "the Supreme Court has ruled that there is a limited constitutional right of privacy based on a number of provisions in the Bill of Rights" (EPIC, 2002:382). The main provision referred to in a number of privacy related Supreme Court cases is the Fourth Amendment (EPIC, 2002:382). This amendment, which addresses search and arrest warrants, states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (Constitutional, 2003:np)

However, third party records, such as consumer marketing profiles or telephone calling records, are generally not protected in this way (EPIC, 2002:382). It is this type of information that the federal government is currently seeking to utilize in order to track down terrorists (Auster, 2003:24).

While established in January 2002, the Information Awareness Office (IAO) within the Defense Advanced Research Projects Agency (DARPA) only began to attract public attention at the end of 2002 (Auster, 2003:24). Led by retired Admiral John Poindexter, the IAO's Total Information Awareness (TIA) project aims to be able to

detect terrorists by tracking their financial footprints (Auster, 2003:24). IAO Deputy Director Robert Popp stated,

> If terror organizations are going to engage in adverse actions against the United States it must involve people and those people will make transactions and those transactions will leave a signature in the information space. (Auster, 2003:24)

However, in order to find "those people" the IAO expects to data mine huge amounts of information about not only potential terrorists, but also innocent Americans. Many fear that sweeping enhancements in data acquisition will lead to the sort of abuses revealed by the Church Committee in 1975 (Wolf, 2001:np). These abuses included a variety of questionable investigative techniques and programs carried out by the FBI and CIA (Wolf, 2001:np). Popp further states, "This is the problem that we face, which is really, really hard. You don't necessarily know a priori the bad guy. That's where you run into the issue of privacy" (Auster, 2003:26).

Thus, it becomes necessary to balance the effort to identify terrorists operating within the United States against possible infringements on the privacy rights of innocent Americans. Whatever steps are taken, the impact of this infringement on privacy should not outweigh the increase it provides in the capability to detect terrorist threats.

4.5.2 Freedom from Discrimination

The prevention of terrorism requires decisive action by law enforcement, the military, and other government agencies. The military actions carried out in Afghanistan, for example, played a vital role in combating the Taliban terrorist network. However, such actions, particularly when targeted at foreign terrorists, may potentially enhance

worldwide prejudices. United Nations High Commissioner for Human Rights, Sergio Vieira de Mello, addressed the rise in discrimination against Muslims by stating, "Arabs and Muslims at large are experiencing increasing incidents of racial discrimination …Singling out, finger pointing and…even in some instances (violence)" (War on Terror, 2002:1). The USA PATRIOT Act states that these acts of violence "should be and are condemned by all Americans who value freedom" (107th Congress, 2001:np). The Act further states that,

> the civil rights and civil liberties of all Americans, including Arab Americans, Muslim Americans, and Americans from South Asia, must be protected, and that every effort must be taken to preserve their safety. (107th Congress, 2001:np)

In addition, many fear that the "war on terror" has led to racial or ethnic profiling of foreigners and cultural groups within the United States (Cole, 2002:1). Since September 11th, thousands of immigrants and foreign citizens have been detained and interviewed as part of the subsequent investigation (Cole, 2002:1-2). An array of pundits have compared these detentions to the internment of U.S. citizens of Japanese descent during World War II. Though the Bush Administration has repeatedly spoken out against racial profiling and insisted that these individuals were suspected terrorists, some argue that their selection was based solely on their country of origin (Cole, 2002:2).

Though every effort must be made to prevent terrorism within the United States, the federal government must be wary of the potential discriminatory nature of certain homeland security actions. Many actions could increase the security of the nation, but their capability to aggravate existing prejudices or implicate racial or ethnic profiling

might make them unacceptable to the American public. We cannot secure the nation by denying the rights that define the nation.

4.5.3 Judicial Rights

Just as it is vital that the federal government avoid unlawfully discriminating against individuals based on their racial or ethnic background, it is equally important that suspected or indicted terrorists not be denied the judicial rights promised them by law. The ongoing detention of individuals implicated in the terrorist attacks on 9/11 and in other terrorist activity has raised concern over whether the federal government has violated certain constitutional rights.

Current concerns include the legality of detentions, access to legal representation, attorney-client privileges, and the right to a fair trial. The denial of these rights to individuals designated as "enemy combatants" has compelled some to accuse President Bush of "usurping powers not conferred on him by the constitution and of infringing on individual freedoms" (Lane, 2002:1). Still, others defend the Administration's stance on preventing terrorism. Former Attorney General William Barr stated, "We shouldn't lose sight of the fact that the way 9/11 affects our civil liberties comes not from the government's response but from the danger caused by terrorists in the first place" (Lane, 2002:2). In fact, much of the government's response, such as denying access to U.S. courts for terrorist detainees in Guantanamo, Cuba, has been upheld by either Congress or the court system (Lane, 2002:2).

Similar to the Fourth Amendment rights potentially denied by new methods of collecting information about terrorists, Fifth and Sixth Amendment rights may be impacted by efforts to bring terrorists to justice. The Fifth Amendment, which addresses rights in criminal cases, states,

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation. (Constitutional, 2003:np)

The Sixth Amendment, which addresses rights to a fair trial, states,

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense. (Constitutional, 2003:np)

These two amendments dictate rights promised Americans by law. Thus, it is vital that all those who are entitled these rights receive them. The question of who is and is not promised these rights, however, is in dispute.

Much of the dispute stems from the distinction between a material witness and a visa violator (Liptak, 2002:6). Because the majority of the detainees were held on immigration charges, the courtrooms were closed for these cases (Liptak, 2002:3). This was justified by pointing out that immigration hearings are not really trials, but merely administrative functions (Liptak, 2002:5). The distinction is vital because a visa violator does not bring the automatic appointment of a government-paid lawyer (Liptak, 2002:6).

Thus, by labeling suspected terrorists as "enemy combatants" or visa violators, their judicial rights are severing restricted.

The United States government must be careful to ensure that its efforts to reduce the threat of terrorism do not unlawfully limit the rights of suspected terrorists. The right to a fair trial, representation, and other legal considerations should be administered when appropriate. It is this issue of appropriateness that truly embodies the trade-off between security and the rights of potential terrorists. Table 4-3 summarizes the measures developed for the *Civil Liberties* considerations. A more detailed description of each of these measures is delineated in Appendix E.

Table 4-3: Civil Liberties Measures

TITLE	MEASURE UNIT	MEASURE TYPE	LOWER BOUND	UPPER BOUND
Privacy Rights				
Fourth Amendment (Physical)	Potential impact of the strategy on Fourth Amendment rights?	Categorical	No Impact	Potentially Severe Impact
Fourth Amendment (Electronic)	Potential impact of the strategy on Fourth Amendment rights?	Categorical	No Impact	Potentially Severe Impact
Freedom from Discrimination				
Discrimination Issues	Does the proposed strategy present issues with discrimination?	Categorical	No Issues	Potentially Severe Issues
Judicial Rights				
Fifth Amendment	Potential impact of the strategy on Fifth Amendment rights?	Categorical	No Impact	Potential Impact
Sixth Amendment	Potential impact of the strategy on Sixth Amendment rights?	Categorical	No Impact	Potential Impact

4.6 Summary

The security of the homeland from terrorist threats and attacks is one of the most fundamental responsibilities held by the Federal government. However, the execution of this responsibility runs the risk of potentially impacting other fundamental duties; namely avoiding excessive budgetary spending and infringements on civil liberties. The three

hierarchies described in this chapter (Homeland Security, Resource Costs, and Civil Liberties) provide a method for the Federal government to employ in measuring the attainment of the values associated with each individual responsibility, as well as to balance them against one another. Appendix F provides an executive summary of the results of this chapter, along with a detailed example of exactly how the hierarchies can be employed.

5. Conclusions and Recommendations

This chapter provides an overview of the goals set forth for this thesis and discusses how they were accomplished. It concludes by providing recommendations for future research in the continuing effort to secure the American homeland from terrorism.

5.1 Summary

The terrorist attacks on 11 September 2001 forced the topic of homeland security to the forefront of national concern. Though an array of commissions and research groups had warned the nation about the *potential* for attacks within the United States, it was not until this grave day in American history that attention was truly focused. The establishment of the Office of Homeland Security, the development of the National Strategy for Homeland Security, and the creation of the Department of Homeland Security, all within a little over a year of the attacks, exemplifies the concern for the threat to the United States. This threat has been amplified by the pervasive vulnerabilities of the nation's critical infrastructure, the deadly intent of modern terrorists, and the widespread capability of these individuals to obtain weapons of mass destruction and mass disruption. In order to combat this threat, and thus secure the homeland, the United States must have the capability to prevent attacks, reduce critical vulnerabilities, and prepare for the possibility that attacks do occur. However, this complex and poorly defined mission can be difficult to accomplish without the proper clarification of objectives and the ability to evaluate how well alternatives accomplish

those objectives. This thesis has attempted to take a critical step in beginning to address these areas of difficulty.

By employing the Value Focused Thinking (VFT) decision analysis methodology, this study has clearly and comprehensively identified and defined what is valued in the strategic effort to secure the United States from terrorism. A value hierarchy of security objectives was developed through a detailed review and analysis of the relevant literature. Additionally, to maximize the efficacy of this hierarchy, initial evaluation measures were developed that facilitate the assessment of improvements to the Federal government's capability to execute recognized homeland security objectives.

Throughout this work it was acknowledged that the security hierarchy alone would not completely capture the tradeoffs at the root of homeland security decision-making. Enhancements in security have the potential to incur negative impacts in the form of excessive resource costs and worse, possible infringements on civil liberties. Thus, it is vital that all three issues be balanced against one another in the development and evaluation of homeland security strategies. The triad of hierarchies developed in this thesis provides high-level decision-makers with a decision support framework that can be utilized to assist this development and evaluation.

Securing the homeland from terrorism is an extremely important, yet difficult, mission that the United States must make every effort to successfully accomplish. The capability to continually measure the progress of this accomplishment is vital. The allocation of scarce resources must only be applied to those options (i.e. strategies) that have the potential to affectively enhance the security of the nation. This study not only provides a method to evaluate such solutions, but also defines the objectives that newly

developed solutions should be designed to target. It also provides parameterized measures for use in other analyses of homeland security options.

5.2 Recommendations

The following recommendations are provided as guidance for further research in homeland security decision-making. The direction provided in this section will assist in the continuation of the work completed in this research.

5.2.1 Decision-maker and Subject Matter Expert Support

The first step in continuing the work that was accomplished in this thesis is to seek and incorporate the inputs of a wide array of homeland security decision-makers and subject matter experts whose knowledge could be leveraged in validating and continuing the VFT analysis. Due to the scope and limits of this study, the three value hierarchies presented in this research were developed directly from the literature, with limited direct input from high-level homeland security experts. Accordingly, these individuals should be solicited in order to substantiate the values and objectives included in the literature-based hierarchies. In addition to the validation of the work already completed, the relevant subject matter experts would assist in the continuation of the remaining analysis. This would be most effectively accomplished with appropriate, visible senior-level support and approval.

In completing the analysis in this study, the primary benefit of decision-maker and subject matter expert support is the ability to stimulate *specific* target capabilities and

minimum requirements that accurately reflect the specific capability condition. Such expertise would provide well-defined endpoints to the currently parameterized functions. In addition, access to the proper high-level decision-makers would provide the insight necessary to weight the value hierarchies. It has been recognized throughout this research that the values that comprise the three hierarchies may not be of equal importance in the eyes of high-level decision-makers. With their support and input, the values could be assigned the appropriate levels of significance. The validation of the three hierarchies, the development of decision-maker specific parameters for measures, and the solicitation of weighting would provide the support necessary to construct a completely operational value model.

With a complete value model, the Federal government would have the capability to help evaluate and rank newly developed homeland security strategies. This ranking would be based on the aspects that are valued in the homeland security decision context and would provide an objective, defendable, and repeatable method to support the allocation of federal resources. While the final decisions on such grave national issues will always require the considered inputs of the branches of government, such a model could aid in screening strategies and identifying "value gaps" in present proposals. In addition to screening alternatives, the complete value model would allow for sensitivity analysis of the established weighting. This type of analysis would provide insight regarding the change in alternative rankings given various changes in weighting.

Though the triad of hierarchies presented in this thesis constitutes great strides toward providing structure to the homeland security decision problem, the support of the relevant decision-makers and subject matter experts, at the appropriate level of authority,

would enhance its contribution. Given the scope of this research (the federal level of government), these individuals may be difficult to acquire for any significant period of time. However, this research has generated interest at a high national level and an executive summary will be provided to the appropriate personnel. The support they could offer would provide a great deal of insight and assist in furthering the usefulness of the value model.

5.2.2 State and Local Governments, and the Private Sector

This thesis chose to address homeland security objectives and capabilities at the federal level of government. Because the defense of the American people is a constitutionally defined responsibility, a method for assessing strategies at the federal level is vital. On the other hand, state and local governments, as well as the private sector, also have homeland security responsibilities. Local first responders and state emergency response personnel are vital in the effort to minimize the damage of terrorist attacks. Additionally, because over 80% of the nation's critical infrastructure is owned and operated by non-government entities, the private sector must allocate scarce resources in the reduction of America's vulnerabilities. Consequently, further research could contribute significantly to homeland security decision support by performing similar studies at these levels of authority. As one example, Captain Quincy Meade developed a decision support structure for the Dayton International Airport to utilize in its effort to enhance security. The integration of this type of analysis with the analysis performed in this thesis would provide the United States with a truly *national* capability

to support decision-making in the homeland security context. The development of a hierarchy of hierarchies would incorporate the decentralized decision-making of state and local governments with the values held at the federal level.

5.2.3 Vulnerabilities versus Susceptibilities

The threat model described in this thesis utilized *Vulnerabilities* as a component of the terrorist threat to the United States homeland. Recall, this model stated:

Vulnerabilities x Intentions x Capabilities = Threat.

However, this expression does not address the fundamental difference between *vulnerabilities* and *susceptibilities*. In fact, as stated in Chapter 1, JP 1-02 uses the word susceptibility in order to define vulnerability (JP 1-02, 2001:464). Homeland security doctrine does not appear to make a clear delineation between the two concepts. In reality, by many definitions, a vulnerability inherently includes the capability of an enemy (Ball, 1998:26, DOD 5000.2-R, 2001: AP3.2.5). Thus, the terms *Vulnerabilities* and *Capabilities* in the threat model would exhibit some redundancy. The Live Fire Test and Evaluation Mandatory Procedures & Reports Section of DoD Regulation 5000.2-R defines susceptibility as, "The degree to which a weapon system is open to effective attack due to one or more inherent weakness" (DOD 5000.2-R, 2001: AP3.2.7). Susceptibility is thus the more accurate term for describing weaknesses that may or may not have the potential (i.e. capability) to be exploited. This same definition can be applied to the nation and its weaknesses to terrorist attack.

Further studies may choose to utilize the alternative threat model shown below.

Susceptibilities x Intentions x Capabilities = Threat.

It should be noted that the vital concept of vulnerability has not been removed from the model. The above equation is robust enough to address both susceptibilities and vulnerabilities. As previously stated, a vulnerability is simply a susceptibility coupled with an existing capability to exploit that inherent weakness. The United States may have a plethora of susceptibilities, but only a subset of them are vulnerabilities subject to exploitation. Thus, the *Susceptibilities x Capabilities* portion of the model represents the nation's vulnerability to terrorism.

This recommendation is not meant to invalidate the research performed with the original threat model. In contrast, it is merely meant to point out the fundamental difference between two interrelated concepts. Realistically, homeland security decision-makers would place priority on reducing those weaknesses that have a known capability to be exploited (i.e. vulnerabilities). Thus, the reduction of vulnerabilities is vital. On the other hand, if the United States chooses to ignore those weaknesses that are currently incapable of being exploited (i.e. susceptibilities), they will eventually become tomorrow's vulnerabilities. Though they are of an admittedly lower priority in today's complex threat environment, the nation's *susceptibilities* should not be completely ignored. Accordingly, future research would be well advised to address this issue in more detail.

5.3 Conclusion

This thesis has only begun to scratch the surface of the complex and pervasive problem of securing the American homeland from terrorist threats and attacks. As long as the critical infrastructures and key assets of the United States remain vulnerable, and terrorists are capable of executing their deadly intentions, homeland security will be of imminent concern. The value hierarchies presented in this study, because they are developed from the objectives defined in homeland security doctrine, provide insight into the difficult process of allocating resources to the development of effective strategy. This insight provides a foundation for the Federal government to leverage in the continuing effort to accomplish one of the most vital missions facing the United States of America; homeland security.

Appendix A: Weighting the Value Hierarchy

Once SDVFs have been created for each evaluation measure, the hierarchy must be weighted. The need for weighting stems from the fact that each objective and evaluation measure may not be equally important to the decision-maker. Rather than simply summing the SDVF scores and calculating an equally weighted average, each evaluation measure receives a weight indicative of its relative importance. By doing this, the scoring of alternatives is more representative of the value-tradeoffs inherent in the decision problem. There are two general methods for weighting a value hierarchy: *global* and *local*.

Global Weighting

Global weighting is performed by assigning each evaluation measure a weight such that all the evaluation measure weights sum to one across their tier. These global weights can then be used to calculate global and local weights for objectives higher up in the hierarchy. The six evaluation measures in the example hierarchy in Figure A-1 have been globally weighted.

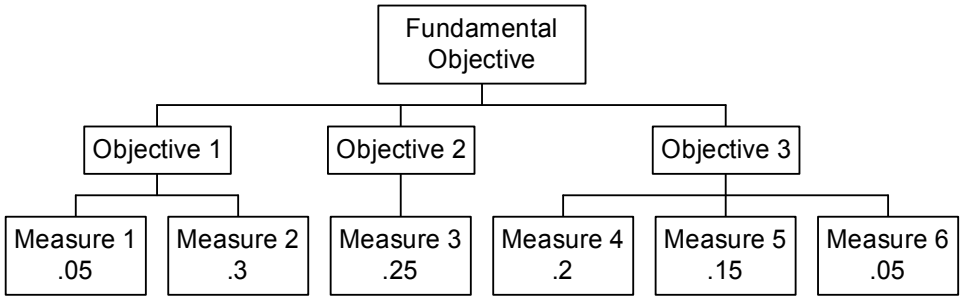

Figure A-1: Globally Weighted Hierarchy

As is required, the global weights across the entire tier sum to one. The global weights for the three associated objectives can be calculated by simply summing the weights of their descendent evaluation measures (e.g. .35 = .05 + .3 for Objective 1 below). These weights are displayed in Figure A-2.

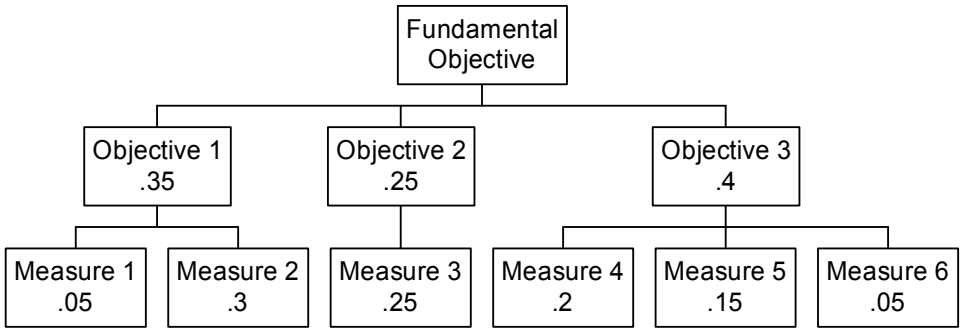

Figure A-2: Global weights of Globally Weighted Hierarchy

Once again, it is important to note that the global weights across each tier sum to one. In the case of the tier with the three objectives (known as the *first* tier), the global weights are the same as the local weights. In fact, in any hierarchy, the local and global weights will be equivalent for the first tier objectives. Furthermore, the global weighting performed on the evaluation measures can be used to calculate local weights for every measure and objective in the hierarchy.

Local weights can be calculated by dividing the global weight of any measure or objective by the total of all the global weights in that particular branch, on that particular tier. For the example hierarchy, the local weight for Measure 1 was calculated by dividing its global weight (.05) by the sum of the global weights in the first branch of the second tier (.05 + .3). The local weights for each objective and measure are shown below.

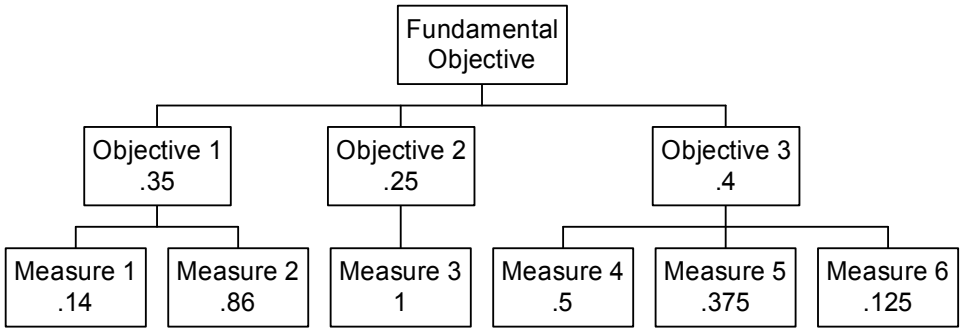

Figure A-3: Local Weights of Globally Weighted Hierarchy

Unlike global weights, local weights sum to one only within a given branch of a tier. If only one objective or measure exists in a branch of a particular tier, such as Measure 3, then the local weight is equal to one. However, calculating local weights from a globally weighted hierarchy is fundamentally different from actually weighting the hierarchy locally.

Local Weighting

When a hierarchy is locally weighted, the weights are assessed for the upper most objectives first (Chambal, 2002:np). Once the first tier has been weighted, each successive tier is weighted one branch at a time. After every objective and measure has been weighted, the global weights can be calculated from the local weights. Figure A-4 shows a hierarchy that has been locally weighted for each branch on each tier.

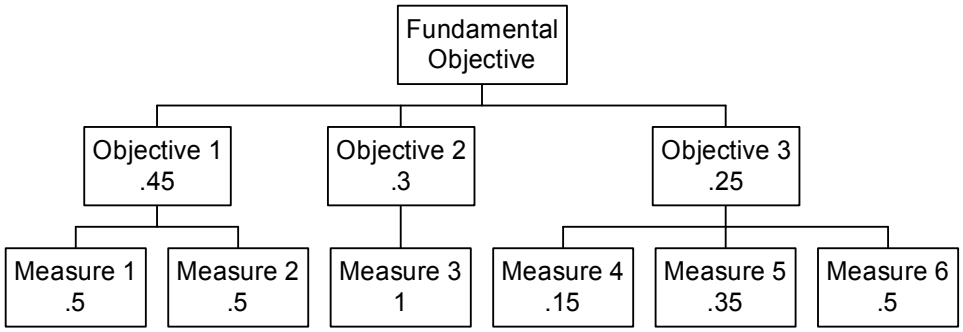

Figure A-4: Locally Weighted Hierarchy

As was stated earlier, the weights on a tier within a branch must sum to one for local weights. Global weights can now be calculated by multiplying the local weight for a given objective or measure by the local weight of the associated objective in the preceding tier. For example, the global weight for Measure 1 would be calculated by multiplying its local weight (.5) by the local weight of Objective 1 (.45). The global weights for this hierarchy are shown in Figure A-5.

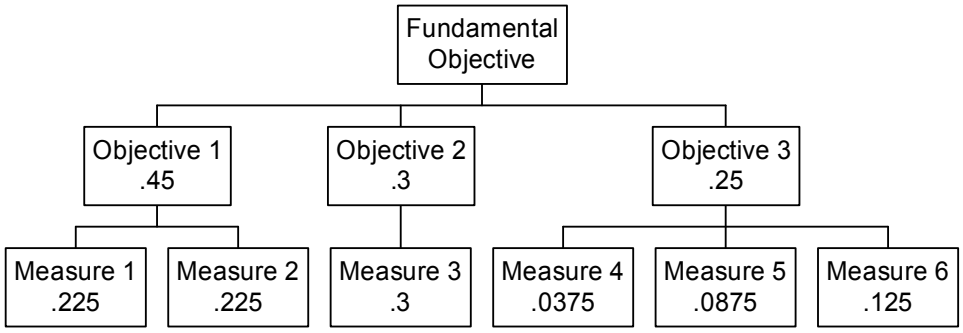

Figure A-5: Global Weights of Locally Weighted Hierarchy

Once again, it is important to note that, even though the hierarchy was locally weighted, the global weights for all the evaluation measures still sum to one.

Selecting a Method to Weight

Whether a hierarchy is weighted globally or locally, it is necessary to calculate the global weights of the evaluation measures in order to score generated alternatives. When considering whether to weight a value hierarchy globally or locally, research performed at AFIT suggests that the hierarchy be weighted in the same manner it was developed (Kahraman, 2002). In other words, if the hierarchy was developed from the evaluation measures (bottom up), then it should be weighted from the bottom up (globally). On the other hand, if the hierarchy began with the fundamental objective and worked down (top down), then it should be weighted in the same manner it was specified (locally). Not only does this method make logical sense, but also it normally results in a more accurate representation of the decision-maker's values (Chambal, 2002:np). Once the decision has been made to weight globally or locally, it is still necessary to select a method for soliciting the weights from the decision-maker.

The two most general methods for determining weights are *swing weighting* and the *"100 marble"* method (Chambal, 2002:np). To assess swing weights globally, the decision-maker must consider how much they value increasing the evaluation measure from its least preferred state to its most preferred (Kirkwood, 1997:70). According to this assessment, the measures are ordered from least to most valued and expressed as a multiple of the least valued measure (Kirkwood, 1997:70). The sum of these multiples is then set equal to 1 and solved to determine each of the weights (Kirkwood, 1997:70). A similar method can be utilized to assess swing weights on objectives rather than evaluation measures (Chambal, 2002:np). In this case, the decision-maker simply orders

the objectives of interest from least to most important. As with the previous method, the objectives are then expressed as a multiple of the least important objective, the sum set equal to one, and the equation solved to determine all the weights. This allows the swing weighting method to be applied to a locally weighted hierarchy.

The second, more direct method for soliciting weights from a decision-maker or group of decision-makers is the "100 marble" method. With this method, the individual or group spreads 100 "marbles" among the objectives or measures of interest (Chambal, 2002:np). The assignment of "marbles" then becomes the weight for the given objective or measure. For example, if an objective received 35 of the 100 "marbles," then its weight would be .35. In situations where the solicitation involves a group of decision-makers, the weights can be averaged, discussed, and recalculated until a consensus is reached (Chambal, 2002:np).

Regardless of how the hierarchy is weighted or how the weights are solicited, the expression of preferences obtained from this process is vital to accurately evaluating alternative solutions to the decision problem.

Appendix B: Affinity Grouping of Homeland Security Objectives

For this research, the issues and initiatives pertaining to homeland security were obtained from the literature. In particular, a content analysis was performed on the following five prominent homeland security documents to obtain a vast collection of ideas and concepts (Stemler, 2001).

- *The National Strategy for Homeland Security*, released by the Office of Homeland Security
- *The Department of Homeland Security*, released by President Bush
- *Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council*
- *Securing the Homeland Strengthening the Nation*, budget released by President Bush
- *Homeland Security: The Strategic Cycle*, released by the ANSER Institute for Homeland Security

This analysis led to the extraction of **363 objectives** related to securing the homeland from terrorist threats and attacks. Using this collection of homeland security objectives, common themes and issues were grouped together to form a hierarchical structure. This method not only assists in the completion of the value hierarchy, but also provides quantifiable support for the values that are included. All 363 of the objectives extracted from the literature are included in this appendix, along with their appropriate grouping.

Key:

ANSER:	*Homeland Security: The Strategic Cycle*, released by the ANSER Institute for Homeland Security
DHS*:*	*The Department of Homeland Security*, released by President Bush
EO 13228:	*Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council*
National Strategy:	*The National Strategy for Homeland Security*, released by the Office of Homeland Security
Budget:	*Securing the Homeland Strengthening the Nation*, budget released by President Bush

Prevention

DHS
- take or effect appropriate preventive action

Threat Detection

Collection

ANSER
- investigate (law enforcement) impending or actual attacks

DHS
- investigate promptly
- identify foreign terrorists
- identify current and future threats to the homeland

EO 13228
- coordinate and prioritize the requirements for foreign intelligence
- ensure sufficient technological capabilities and resources to collect intelligence
- investigate terrorist threats and attacks
- facilitate collection of threat information from State and local governments
- identify priorities and coordinate efforts for collection of information

National Strategy
- Ensure prompt investigation of possible terrorist activity
- Identify items that have terrorist applications and legitimate commercial applications
- Evaluate and study mechanisms for reporting suspect purchases
- Establish a consolidated terrorist watch list
- Obtain identifying information on known or suspected terrorists for databases
- Investigate both suspected and confirmed terrorist activity
- Increase counterterrorism investigative capabilities and flexibility
- Investigate suspicious financial transactions
- Recognize harmful dual-use chemicals
- Develop Joint Terrorism Task Forces with operational responsibility for terrorism investigations not related to ongoing prosecutions
- Investigate criminal rings that produce false documents
- Uncover terrorist financing

Analysis

ANSER
- remove the anonymity that provides security for terrorists

DHS
- fuse and analyze legally accessible information
- assess current and future threats to the homeland
- analyze information in a timely and thorough manner

EO 13228
- identify priorities and coordinate efforts for analysis of information

National Strategy
- Increase the number and capabilities of people analyzing intel
- Evaluate and study mechanisms for analyzing suspect purchases
- Utilize commercially available databases to data mine for patterns of criminal behavior
- Develop predictive models to help identify future illegal financing
- Detect and diagnose bio threats
- Enhance ability to detect terrorist activities at the preparation stage

Dissemination

ANSER
- integrate relevant law enforcement and intelligence efforts
- increase coordination and information exchange among all levels of government

DHS
- ensure sharing of information between databases
- disseminate information in a timely and thorough manner
- convey actionable intelligence and threat information in a coherent and efficient manner

EO 13228
- facilitate the exchange of information among pertinent agencies
- disseminate intelligence as appropriate

National Strategy
- Ensure law enforcement can access information on suspected terrorists
- Expand data included in the FBI National Crime Information Center database
- Include data provided to immigration and consular officers
- Ensure that the "cop on the beat" has access to pertinent information
- Ensure flow of information and knowledge to and from field offices

- Improve collaboration and information sharing with other agencies
- Disseminate information regarding the risk of terrorist acts
- Create common vocabulary, context, and structure about nature of threats
- Combine national and international investigative capacity at federal level with "on the
  beat" knowledge at state and local level
- Ensure participation of law enforcement at all levels and coordination of all relevant
  agencies and officials (in sharing of information about threats)
- Facilitate coordination and communication among agencies with immigration and
  enforcement responsibilities (regarding threats)
- Provide greater security through better intel, coordinated national efforts, and international cooperation

Denial of Entry

Awareness (fourth tier values: Tracking, Screening, and Inspecting)

DHS
- manage who and what enters the homeland
- establish near shore and port domain awareness
- track foreign terrorists

National Strategy
- Enable greater visibility of vehicles, people, and goods coming and going
- Internationally screen and verify security of goods and identity of people before they reach our shores and land borders
- Verify and process the entry of people
- Record the arrival and departure of foreign visitors
- Pre-screen containers before they arrive at U.S. ports
- Develop and deploy new inspection procedures and detection systems
- Identify high-risk shipping containers
- Inspect high-risk shipping containers
- Improve maritime domain awareness
- Detect illegal intrusions
- Detect the transport of nuclear explosives toward our borders and into the U.S.
- Initiate and sustain research and development efforts aimed at new and better passive
  and active detection systems (at the border)
- Propose national standards for screening and background checks
- Track dangerous bio agents
- Increase oversight of pathogens used for bioterrorism

- Improve capability to detect the movement of nuclear materials (toward our borders)

Budget
- screen goods and people prior to arrival in U.S. territory
- track the movement of cargo and the entry and exit of individuals

Control

ANSER
- defend aerospace, maritime, and land borders

DHS
- secure air, land, and sea borders
- prevent the entry of terrorists and instruments of terror
- prevent the importation of nuclear weapons and materials
- exclude agricultural pests and diseases at the border
- verify compliance with entry conditions for all categories of visas
- translate analysis into action in the shortest possible time (keep out known threats)

EO 13228
- prevent the entry of terrorists and terrorist materials
- improve security of U.S. borders, territorial waters, and airspace
- prevent unlawful importation of WMDs

National Strategy
- Control issuance of visas and coordinate border-control activities
- Develop border continuum framed by land, sea, and air dimensions
- Minimize misuse of travel documents
- Ensure USCG has resources necessary to perform its missions
- Ensure full enforcement of the laws that regulate the admission of aliens to the U.S.
- Implement the Enhanced Border Security and Visa Entry Reform Act
- Bar terrorists or terrorist-supporting aliens from the U.S.
- Improve command and control systems, and shore-side facilities
- Apprehend goods and people (who attempt to illegally enter the country)
- Prevent the transport of nuclear explosives toward our borders and into the U.S.
- Regulate the shipment of certain hazardous bio organisms and toxins
- Secure the national airspace
- Translate threat information into appropriate action in the shortest possible time (keep out known threats)

Budget
- provide a strong defense for the American people against all external threats (keep the threat out)
- ensure compliance with entry and import permits
- deny access to individuals who should not enter the U.S.

Threat Reduction

Deterrence

ANSER
- have the policies and posture that deters our enemies from attacking
- have the ability to punish
- reestablish deterrence
- address conditions that give rise to terrorist organizations

National Strategy
- Utilize advance warning to intercede and prevent attacks

Means Denial (fourth tier values: Financial and Logistical)

ANSER
- arms control treaties

EO 13228
- prevent unauthorized access to and development of WMDs (denial of capabilities)

National Strategy
- Pursue individuals who provide logistical support to terrorists
- Target and interdict financing of terrorist operations
- Freeze the accounts of, and seize the assets of individuals and organizations that finance terrorists
- Prevent terrorist use of nuclear weapons (Deny them the capability)
- Dismantle criminal rings that produce false documents
- Prosecute terrorist financing
- Ensure continued strict security for the global inventory of nuclear weapons (denying them the capabilities)
- Secure dangerous bio agents
- Increase security of pathogens used for bioterrorism
- Develop and use smart and secure shipping containers
- Address bio threats (taking action to eliminate the threat)

Action Denial (fourth tier values: Law Enforcement, Military, and Other)

ANSER
- possess the capabilities and associated policies that allow the preemption of attacks
- in preemption, selectively use all elements of national power, to include military force and law enforcement
- eliminate the current threat and the possibility of future attacks by that specific actor
- arrest and prosecute terrorists
- use military force or covert actions

DHS
- disrupt and prevent terrorist acts
- enhance the capability to preempt terrorist plots
- intervene promptly
- translate analysis into action in the shortest possible time (first step in eliminating threat)
- counter potential threats to coasts, ports, and inland waterways

EO 13228
- facilitate removal of terrorists (who have illegally entered the U.S.)

National Strategy
- Track down and deport anyone who has illegally entered the country
- Preempt terrorists flawlessly, especially when WMDs are involved
- Translate threat information into appropriate action in the shortest possible time (first step in eliminating the threat)

Vulnerability Reduction

National Strategy

- Reduce vulnerabilities and adopt best practices
- Reduce the overall risk to our country

Assessment

Identification

DHS
- build a comprehensive assessment of the infrastructure sectors

National Strategy
- Identify critical assets, systems, and functions
- Determine what assets, systems, and functions are critical
- Build a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets

Analysis

DHS
- examine vulnerabilities, test security systems, and evaluate the threat
- map threats against current vulnerabilities
- maintain a comprehensive assessment of the infrastructure sectors

EO 13228
- develop criteria for evaluating security measures (of CI)
- review and assess vaccination policies and stockpiles, and hospital capacities

National Strategy
- Perform comprehensive vulnerability assessments of CI and key assets
- Perform threat-vulnerability integration
- View the U.S. from the perspective of the terrorist (part of the threat/vulnerability process)
- Predict the methods, means, and targets of terrorists (part of the threat/vulnerability process)
- Uncover weaknesses in security measures (of CI)
- Comprehensively assess threats and vulnerabilities across all sectors
- Maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets
- Ensure ability to continuously evaluate threat information against current vulnerabilities
- Comprehensively review CI personnel surety programs
- Comprehensively review other protection measures necessary to deny terrorist access to CI
- Ensure we address vulnerabilities that involve more than one sector (part of the analysis of CI)
- Determine the highest risks
- Evaluate potential effects of attacks

Prioritization

DHS
- develop and harness the best modeling, simulation, and analytic tools to prioritize effort in protecting infrastructure
- place an especially high priority on protecting cyber infrastructure (part of prioritization prior to actually protecting)

National Strategy
- Set priorities for CI protection and "target-hardening"
- Set priorities for long-term protective action and "target-hardening"
- Place an especially high priority on protecting our cyber infrastructure (part of prioritization prior to actually protecting)
- Identify highest priority threat agents to determine which countermeasures are high priority
- Enable decisive near-term action and guide rational long-term investment of protection effort and resources (decisive and rational investment implies prioritization)
- Prioritize effort accordingly (to risks)
- Prioritize critical assets, systems, and functions

Protection

ANSER
- deny terrorists the effects they seek

DHS
- protect the nation's institutions
- protect the U.S. from catastrophic terrorism
- protect significant vulnerabilities
- take or effect appropriate protective action

EO 13228
- strengthen measures for protecting energy services, telecommunications, and other
  critical services
- protect critical information systems
- protect special events
- protect transportation systems
- protect livestock, agriculture, and food and water services
- protect the U.S. and its critical infrastructure from the consequences of terrorist attacks

National Strategy
- Protect critical transportation assets
- Protect a diverse population of all ages and health conditions
- Protect key assets
- Invest accordingly in protecting against potential attacks

Budget
- protect citizens against the threat of bioterrorism
- protect ports and coastal areas

Vigilance

DHS
- issue timely warnings (fundamentally different from *alerting*)
- provide useful warning
- enhance the capability to warn appropriate sectors

National Strategy
- Facilitate and encourage private firms to share important information on the infrastructure they control (to enhance vigilance)
- Enable sharing of essential HLS information between the government and private sector (to enhance vigilance)
- Provide useful warning
- Issue warnings
- Improve infectious disease and chemical terrorism surveillance
- Characterize appropriate levels of vigilance
- Recognize patterns of disease occurrence and identify potential outbreaks (increase vigilance)
- Monitor public and private databases for indicators of bio or chem. Attack
- Strengthen parallel system for monitoring agricultural outbreaks

Budget
- enhance medical communications and disease surveillance capabilities (enhance vigilance)

Readiness

DHS
- coordinate a comprehensive national plan for protecting the nation's infrastructure
- establish policies for standardized, tiered protective measures

National Strategy
- Enable the private sectors ability to carry out its protection responsibilities
- Provide one primary contact for coordinating protection activities
- Facilitate and encourage private firms to share important information on the infrastructure they control (to enhance readiness)
- Enable sharing of essential HLS information between the government and private sector (to enhance readiness)
- Strengthen partnerships among federal, state, local, and private sector (to enhance protection)
- Harness the efforts of agencies with specialized expertise in protecting CI
- Collaborate protection efforts with the private sector which owns 85% of CI
- Inform and facilitate decisions appropriate to different levels of government

- Improve the focus of the Nation's defenses against terrorism
- Consolidate and focus CIP activities
- Develop and coordinate implementation of a comprehensive national plan to protect CI
- Establish standards and benchmarks for CIP
- Provide means to measure CIP performance
- Create incentives for the private sector to adopt security measures
- Empower all Americans to secure the portion of cyberspace that they control (by providing necessary information)
- Enhance our ability to quickly make life-or-death decisions based on the best possible understanding of the consequences
- Advance the state of knowledge in infectious disease prevention, forensic epidemiology, and microbial forensics
- Build a concentrated, national, centralized, and deployable expertise on terrorism issues
- Help individual citizens help themselves
- Characterize appropriate levels of preparedness and readiness

Budget
- invest in U.S. health care system

Surety

DHS
- defend against human, animal, and plant diseases
- invent new vaccines, antidotes, diagnostics, and therapies
- secure America's critical infrastructure
- secure transportation systems
- ensure the safety and security of America's inland waterways, ports, harbors, coastline, and territorial seas
- ensure a robust and efficient transportation infrastructure
- proactively help communities and citizens avoid becoming victims
- focus on risk mitigation by promoting disaster-resistant communities

National Strategy
- Efficiently apply effective transportation security measures
- Upgrade security in all modes of transportation
- Implement unified, national standards for trans. security
- Permanently, physically harden a target or maintain reserve of personnel and equipment that can handle a surge
- Increase the security of global transportation systems and commerce
- Effect action accordingly (security actions after warnings)
- Pursue new defenses that increase efficacy while reducing side effects
- Conduct homeland defense and assist civil authorities

- Perform national defense, maritime safety, maritime mobility, and protection of natural resources
- Establish combat air patrols
- Address the unique security challenges of each CI sector
- Explore systems that can detect whether an individual has been immunized against a threat pathogen
- Work toward development of broad spectrum antivirals to meet the threat of engineered pathogens
- Pursue accelerated FDA approval of safer and effective products

Budget
- develop specific new vaccines, medicines, and diagnostic tests
- provide enhanced defenses for critical high-risk vessels and coastal facilities

Response Preparedness

ANSER
- respond to actual attacks

DHS
- prepare to minimize the damage and recover from attacks
- prepare for and respond to attacks involving WMDs
- ensure preparedness of emergency response professionals

EO 13228
- improve and sustain preparedness
- prepare for the consequences of terrorist attacks

National Strategy
- Prepare to deal with all potential hazards, especially WMDs
- Dramatically improve first responder preparedness for terrorist incidents

Budget
- have capability to respond to WMDs

Damage Minimization

EO 13228
- mitigate the consequences of terrorist attacks (immediate)

Attack Detection

DHS
- develop, deploy, manage, and maintain systems to detect biological attacks
- recognize, identify, and confirm the occurrence of an attack

EO 13228
- develop protocols and equipment to detect the release of WMDs

National Strategy
- Develop, test, and field detection devices and networks that provide immediate and accurate warnings (*alerts*)
- Develop sensitive and highly selective systems that detect the release of bio and chem. agents
- Increase the speed and precision of diagnoses and confirmation of bio attacks
- Create new technologies for detection of WMD attacks
- Quickly recognize and report bio and chem. attacks

Budget
- detect bioterrorist attacks

Rapid Response

ANSER
- mitigate or stop an attack or its effects
- respond to the economic impact of major attacks (immediate)

DHS
- develop and utilize equipment and systems for communication among response personnel
- develop and implement scientific and technological countermeasures to attacks
- reduce loss of property

EO 13228
- ensure readiness and coordinated deployment of response teams
- stabilize U.S. financial markets (immediate response)

National Strategy
- Gather data from all systems, quickly assess the extent of an attack, and recommend response options
- Provide a direct line of authority for response teams
- Obtain and utilize equipment, systems, and procedures that allow response personnel to communicate with one another

- Achieve interoperability with all emergency response bodies
- Prepare to work effectively with each other in emergency response situations
- Provide federal, rapid response and critical surge capacity to support localities
- Evacuate casualties
- Ensure America's ability to respond rapidly to bioterrorism or mass casualty incidents
- Ensure readiness of first responders to work safely in an area exposed to WMDs
- Maintain and expand the national program to prepare volunteers for terrorism-related response support

Budget
- manage bioterrorist attacks

Treatment

ANSER
- restore public health and safety (immediate)

DHS
- reduce loss of life
- minimize the morbidity and mortality caused by attacks

National Strategy
- Plan for receipt and distribution of medicines from national stockpile
- Support equipping of state and local health care personnel to deal with WMDs (first responders)
- Maintain and rapidly distribute strategically located "Push Packs" of medical supplies
- Accelerate the availability of investigational drugs during public health emergencies
- Ensure availability of medical products
- Support training of state and local health care personnel to deal with WMDs (first responders)
- Develop, maintain, and provide information on the health effects of hazardous substances (to better train first responders)
- Advance the state of knowledge in infectious disease treatment (immediate treatment)
- Minimize casualties
- Enable first responders to treat the injured effectively
- Expand surge capacity of hospitals to deal with mass-casualty situations
- Provide medical personnel to care for the injured following an attack (immediately after)

Budget
- train health care providers to handle victims (first responders)
- save lives and limit casualties after an attack
- enhance surge capabilities of health care system (dealing with immediate consequences)
- build up the National Pharmaceutical Stockpile

Containment

EO 13228
- contain WMDs and mitigate the effects of these attacks

National Strategy
- Accurately interpret biosafety containment provisions

Recovery

DHS
- aid America's recovery from attacks
- promote recovery from attacks

Decontamination

EO 13228
- remove WMDs (decontamination)

National Strategy
- Support research into decontamination technologies and procedures
- Require annual certification of first responders to decontaminate any hazard
- Decontaminate affected buildings and neighborhoods
- Create new technologies for cleanup of WMD attacks
- Determine when to permit individuals to re-enter buildings and areas
- Advice public authorities on when it is safe to return to affected areas

Restoration

ANSER
- respond to the economic impact of major attacks (long-term)
- provide emergency relief services to governments, businesses, and individuals (to restore the services they provide)

EO 13228
- ensure rapid restoration of critical infrastructure services and facilities
- ensure rapid restoration of critical information systems
- manage economic and financial consequences (long-term response at national level)

National Strategy
- Provide military police to assist local law enforcement officials following an attack (to restore order)
- Provide assistance in transportation, communication, and logistics following an attack

Reconstruction

- by National Strategy definition

Assistance (fourth tier values: Medical, Financial, and Logistical)

ANSER
- restore public health and safety (long-term)
- provide emergency relief services to governments, businesses, and individuals (to assist with losses caused by attack)

EO 13228
- provide medical, financial, and other assistance to victims (long-term assistance)

National Strategy
- Test whether illnesses or complaints are attributable to WMD exposure (long-term medical treatment)
- Assist the victims of terrorist attacks, and their families, and others indirectly affected (long-term assistance)
- Offer crisis counseling, cash grants, low-interest loans, unemployment benefits, free
  legal counseling, and tax refunds
- Advance the state of knowledge in infectious disease treatment (long-term treatment)

Budget
- train health care providers to handle victims (long-term treatment)

Appendix C: Homeland Security Hierarchy Definitions

Figure C-1 displays the complete homeland security value hierarchy that was presented in Chapter 4.

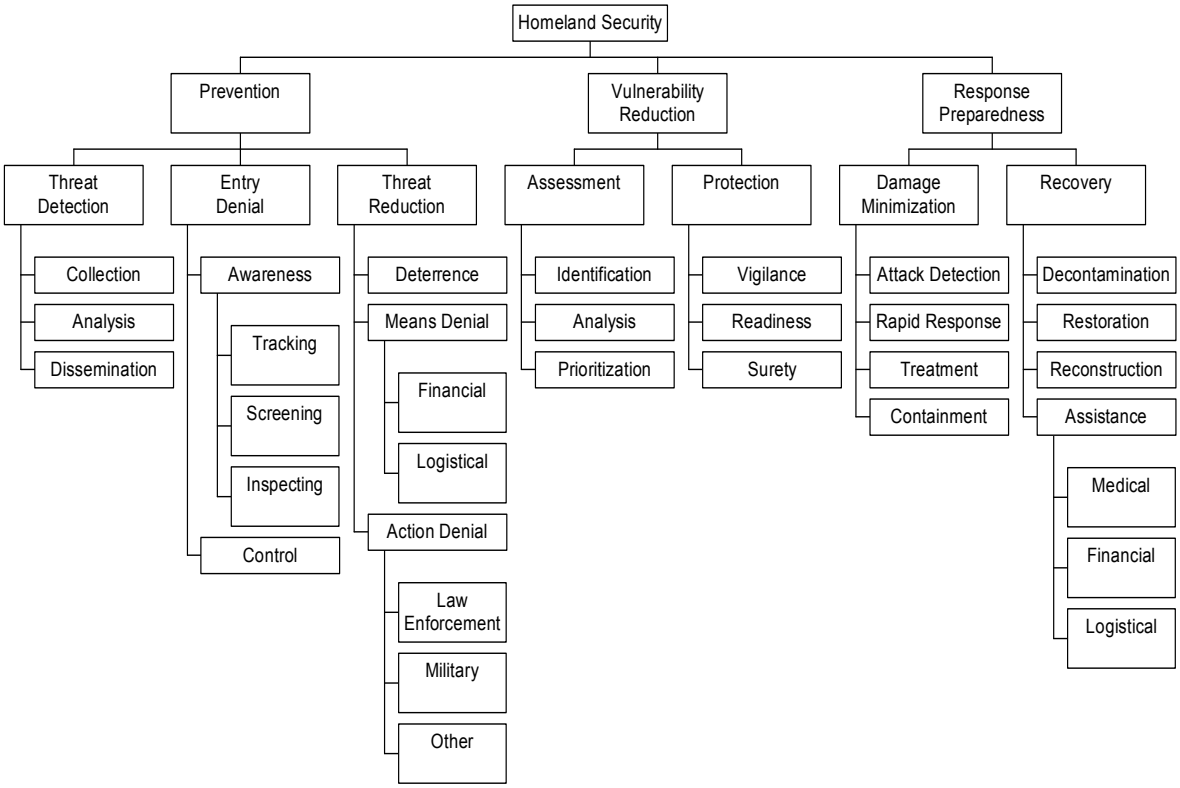

Figure C-1: Homeland Security Hierarchy

Prevention

Figure C-2 displays the *Prevention* branch of the larger homeland security hierarchy presented in Figure C-1.

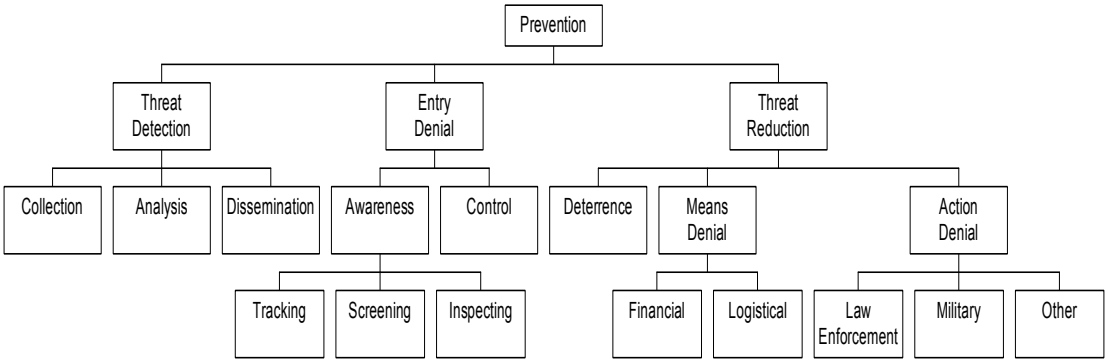

Figure C-2: Prevention Branch of Security Hierarchy

These values are further clarified in the definitions in Tables C-1 through C-7.

First Tier Definitions

Table C-1: Prevention Value Definitions

Prevention Value Definitions
Threat Detection**:* The timely and thorough collection, analysis, and dissemination of information and intelligence regarding terrorist threats located both within the United States and abroad. (developed from EO 13228:1; DHS:14) ***Entry Denial: Actions undertaken to increase the awareness and control of who and what is entering the United States. (developed from NS:22-23)
***Threat Reduction**:* Actions at home and abroad, aimed at deterring known or potential terrorists and denying them the capabilities necessary to carry out attacks on the United States. (developed from ANSER:1; NS:26,38; EO 13228:3)

Second Tier Definitions

Table C-2: Threat Detection Value Definitions

Threat Detection Value Definitions
Collection: The obtaining of information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources. (JP 1-02:76)
Analysis: The conversion of information into intelligence through the integration, evaluation, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (modified from JP 1-02:217)
Dissemination: The delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (JP 1-02:217)

Table C-3: Entry Denial Value Definitions

Entry Denial Value Definitions
Awareness: The tracking, screening, and inspection of goods and people prior to their entry into the United States. (developed from Budget:16; NS:22-23)
Control: Defensive actions undertaken to deny access to goods and people that should not enter the United States. (developed from Budget:17-18; NS:22)

Table C-4: Threat Reduction Value Definitions

Threat Reduction Value Definitions
Deterrence: The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (JP 1-02:129)
Means Denial: Actions undertaken to impede or prevent access to the financial and logistical support necessary to facilitate terrorist operations. (developed from EO 13228:3; NS:26,28,38)
Action Denial: Law enforcement, military, and other preemptive or retaliatory actions targeted at terrorists and their supporters. (developed from ANSER:1,3; DHS:14; NS:43)

Third Tier Definitions

Table C-5: Awareness Value Definitions

Awareness Value Definitions
Tracking: The capability to maintain and record the location and activities of people and goods. (developed from DHS:14; NS:23,28,40; Budget:16)
Screening: The capability to observe, identify, and report information pertaining to people and goods. (developed from JP 1-02:385; NS:22; Budget:16)
Inspecting: The capability to physically verify the security of people and goods. (developed from JP 1-02:215; NS:22-23)

Table C-6: Means Denial Value Definitions

Means Denial Value Definitions
Financial: Actions undertaken to impede or prevent access to the financial support necessary to facilitate terrorist operations. (developed from EO 13228:3; NS:26,28,38)
Logistical: Actions undertaken to impede or prevent access to the logistical support necessary to facilitate terrorist operations. (developed from EO 13228:3; NS:26,28,38)

Table C-7: Action Denial Value Definitions

Action Denial Value Definitions
Law Enforcement: Law enforcement preemptive or retaliatory actions targeted at terrorists and their supporters. (developed from ANSER:1,3; DHS:14; NS:43)
Military: Military preemptive or retaliatory actions targeted at terrorists and their supporters. (developed from ANSER:1,3; DHS:14; NS:43)
Other: Preemptive or retaliatory actions conducted by other authorized agencies and organizations targeted at terrorists and their supporters. (developed from ANSER:1,3)

Vulnerability Reduction

Figure C-3 displays the *Vulnerability Reduction* branch of the larger homeland security hierarchy presented in Figure C-1.

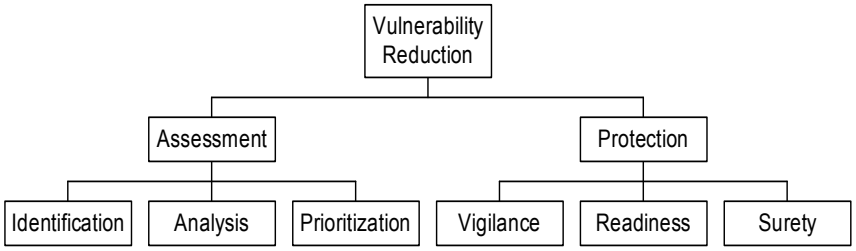

Figure C-3: Vulnerability Reduction Branch of Security Hierarchy

These values are further clarified in the definitions in Tables C-8 through C-10.

First Tier Definitions

Table C-8: Vulnerability Reduction Value Definitions

Vulnerability Reduction Value Definitions
***Assessment**:* The identification, analysis, and prioritization of America's critical infrastructure and key assets, based on associated vulnerabilities. This comprises the evaluation of those people, systems, symbols, facilities, functions, and events, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating impact on national security, governance, public health and safety, economy, and morale. (developed from NS:2,29-30,33-34; DHS:15)
***Protection**:* Actions undertaken to increase the vigilance, readiness, and surety of America's critical infrastructure and key assets. These defensive efforts occur subsequent to vulnerability-based assessments. (developed from NS:18,23,34)

Second Tier Definitions

Table C-9: Assessment Value Definitions

Assessment Value Definitions
Identification: The determination of which people, systems, symbols, facilities, functions, and events are critical to national security, governance, public health and safety, economy, and morale. (developed from NS:29-30,33-34)
Analysis: The review and evaluation of critical infrastructure and key assets, including the mapping of threat information against current vulnerabilities. (developed from NS:33-34; DHS:3,14)
Prioritization: The establishment of priority for efforts and resources invested in protecting critical infrastructure and key assets. (developed from DHS:15; NS:33-34)

Table C-10: Protection Value Definitions

Protection Value Definitions
Vigilance: Actions undertaken to increase the appropriate critical infrastructure sectors' and population's awareness and watchfulness regarding recognized threats and vulnerabilities. (developed from DHS:3,14; NS:13,16,18)
Readiness: The establishment of contingency plans, policies, and standards to ensure the ability of critical infrastructure sectors to deliver the key services for which they were designed. (developed from DHS:15; NS:33; JP 1-02:362)
Surety: Physical and cyber measures designed to prevent unauthorized access to critical infrastructure and key assets, and to safeguard them against loss or damage. (developed from DHS:15; NS:33-34; JP 1-02:335)

Response Preparedness

Figure C-4 displays the *Response Preparedness* branch of the larger homeland security hierarchy presented in Figure C-1.

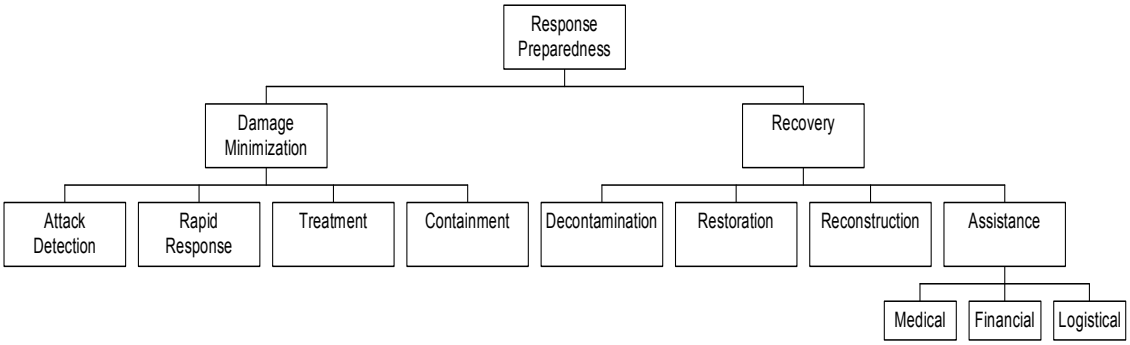

Figure C-4: Response Preparedness Branch of Security Hierarchy

These values are further clarified in the definitions in Tables C-11 through C-14.

First Tier Definitions

Table C-11: Response Preparedness Value Definitions

Response Preparedness Value Definitions
***Damage Minimization**:* The capability to detect a terrorist attack, respond rapidly, treat those who are harmed, and contain the damage. (developed from NS:3,38)
***Recovery**:* The capability to decontaminate the attack site, rapidly restore vital systems and services, rebuild destroyed property, and assist victims following a terrorist attack. (developed from NS:3,38-39)

Second Tier Definitions

Table C-12: Damage Minimization Value Definitions

Damage Minimization Value Definitions
Attack Detection: The capability to identify, recognize, confirm, and report the occurrence of a terrorist attack. (developed from DHS:12; NS:38)
Rapid Response: The capability to quickly assess the extent of an attack, recommend response options, and deploy response teams in order to mitigate the impact of an attack. (developed from NS:39; EO 13228:2)
Treatment: The capability of health care providers to save life and limb and stabilize victims of terrorist attacks sufficiently to withstand evacuation to the next level of care. (modified from JP 1-02:167) ***Containment:*** The capability to stop, hold, or surround the effects of terrorist attacks and to prevent the spread of any part of the attack for use elsewhere. (modified from JP 1-02:94)

Table C-13: Recovery Value Definitions

Recovery Value Definitions
Decontamination: The capability to make any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing the effects of a terrorist attack. (modified from JP 1-02:120)
Restoration: The capability to reestablish the operational abilities of critical infrastructure systems and services affected by terrorist attacks. (developed from EO 13228:3)
Reconstruction: The capability to restore an item to a standard as nearly as possible to its original condition in appearance, performance, and life expectancy. (modified from JP 1-02:364)
Assistance: The capability to provide long-term medical, financial, and logistical aid to victims of terrorist attacks. (developed from EO 13228:3; NS:45)

Third Tier Definitions

Table C-14: Assistance Value Definitions

Assistance Value Definitions
Medical: The capability to provide long-term medical aid to victims of terrorist attacks. (developed from EO 13228:3; NS:45)
Financial: The capability to provide long-term financial aid to victims of terrorist attacks. (developed from EO 13228:3; NS:45)
Logistical: The capability to provide long-term logistical aid to victims of terrorist attacks. (developed from EO 13228:3; NS:45)

Introduction

This appendix discusses an array of issues that homeland security decision-makers might consider in the development of minimum requirements and target capability levels for each of the objectives associated with the 29 lowest tier values presented in Figure D-1.

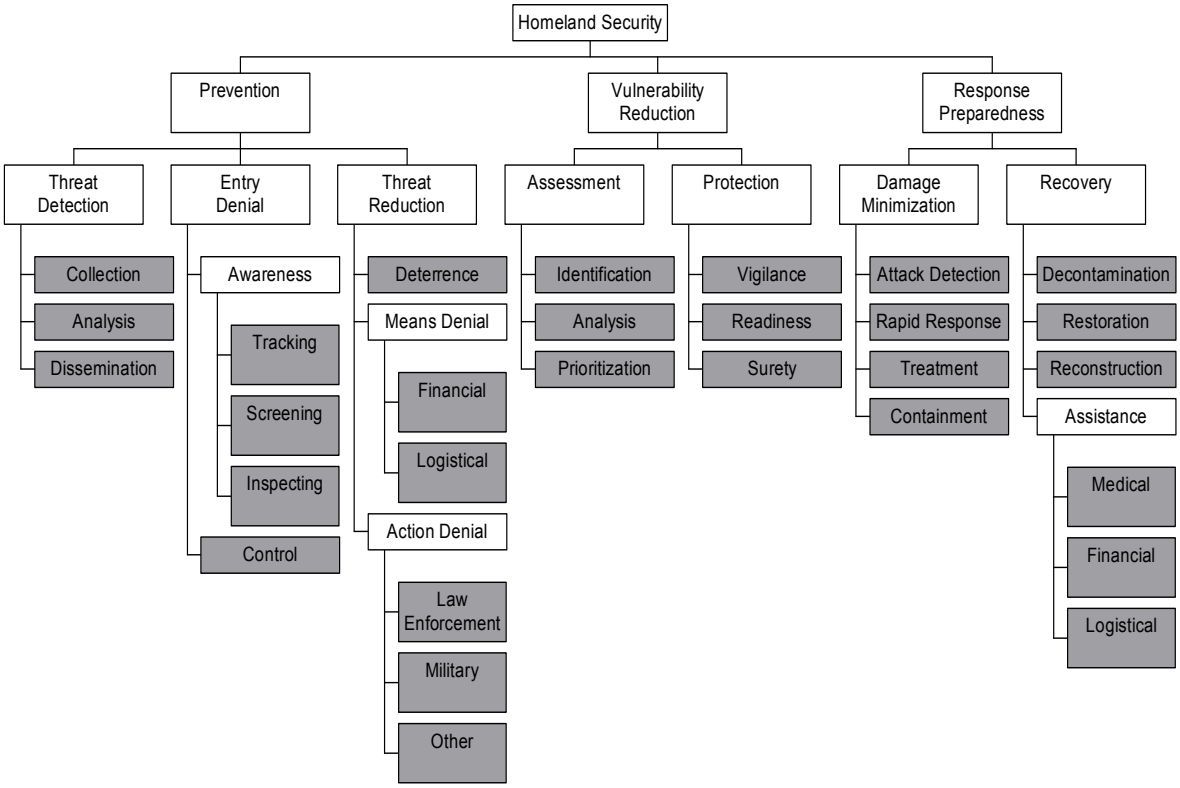

Figure D-1: Homeland Security Value Hierarchy

The capability to execute these objectives is vital to the security of the homeland. Thus, newly developed strategies should target the improvement of these capabilities.

Consequently, this study assesses improvements to the nation's critical homeland security capabilities as a means to measure the values presented in Figure D-1. Recall, the measurement of value is achieved with the following equations.

$$V_i(x) = \begin{cases} 1, & \text{for } C_i = 100 \\ \dfrac{x}{100}, & \text{for } C_i = 50 \\ \dfrac{1 - e^{-x \cdot R}}{1 - e^{-100 \cdot R}}, & \text{otherwise} \end{cases}$$

where $$R = \frac{50 - C_i}{\rho}, \quad \text{for } \rho > 0.$$

These equations are parameterized by current capability (C_i). It is, therefore, vital that current capability is accurately identified in each area. The ideas discussed in this appendix provide the necessary foundation for Federal level decision-makers to define desired and minimum acceptable levels of capability that subsequently provide the framework to identify current capability.

Prevention Measures

This section delineates the topics and issues that might be considered when developing the capability continuums for the thirteen critical objectives depicted in the *Prevention* branch of the hierarchy in Figure D-1.

Collection

The capability to obtain useful information about terrorist threats is vital. This information might be attained from direct observation or from the solicitation of a variety of official, unofficial, and public sources. The purpose of this vast collection of data is to assist in the effort to develop actionable intelligence that can be utilized by a variety of agencies and organizations. Thus, the more information the Federal government can obtain, the more resources it will have to develop intelligence. However, raw data is not enough. This information must be relevant to the mission at hand; preventing terrorism. If the data collected does not support the information needs of the war against terrorism, then its usefulness will be limited. Additionally, the information must be obtained in a timely enough manner to facilitate its analysis and development into intelligence.

The appropriate subject matter experts (SMEs) will be needed to define the target amount of information that needs to be collected, as well as the context of the data. This target level should parallel the amount of information necessary to attain the desired level of threat detection. Similarly, SMEs should define attainable time horizons between the recognition of need for data and its attainment. In addition to the target level, it will be necessary to define a minimum acceptable level of data collection. The Federal government must perform some level of threat detection just to stay abreast of the most obvious threats. Certain types on information will always need to be obtained merely to achieve a noticeable resemblance of detection. This should be considered in the development of minimum requirements.

Analysis

The nation must also have the capability to analyze the data that is collected about terrorist threats. This information must be integrated, evaluated, and interpreted in order to convert it into useful intelligence. It was previously stated that the more information the Federal government can obtain, the more resources it will have to develop intelligence. Thus, it is logical that the Federal government would also value the capability to synthesize as much data as possible. Whether this involves greater numbers of personnel or more advanced technological capabilities, efforts should be made to increase the amount and speed of analysis and creation of intelligence.

Again, knowledgeable SMEs will be needed to define the target amount and speed of information integration, evaluation, and interpretation. When the need is recognized, collected information must be converted to actionable intelligence as quickly as is necessary to facilitate preventative activities. In contrast, SMEs must also define the minimum amount of intelligence that would be needed to maintain an acceptable detection capability. These definitions will largely be driven by the needs of the organizations and agencies that require the intelligence.

Dissemination

For developed intelligence to be applied to the prevention of terrorism, it must be made available to the appropriate agencies and organizations. If this information is not shared with the entities responsible for reducing the threat, then it is of limited use. The needs of varying entities, however, may be dissimilar. Accordingly, it is vital that

agencies and organizations be provided with the amount of intelligence they deem necessary to accomplish their mission. At the same time, the entities that are delivering the intelligence must take into account the sensitivity of the information in question. In general, the Federal government should make every effort to disseminate as much of the required intelligence as is reasonably possible.

It will be up to the SMEs to clarify what is reasonable. Ideally, the target level would be to provide every homeland security agency or organization with 100% of the intelligence they require to accomplish their mission. However, the classification of various types of information may make this unacceptable. Consequently, well-informed SMEs must define the desired level of information sharing that the Federal government should pursue. Such sharing may initially be done electronically using artificial intelligence and neural net approaches. When a critical level of correlations is attained, the system might flag the relations and suggest a review by appropriate experts. Furthermore, because a complete lack of dissemination would leave some in the blind, a minimum amount of intelligence delivery must be defined. Preventative agencies and organizations must be provided with at least some portion of the information they request.

Tracking

In order to deny terrorist threats access to the United States, the Federal government must be aware of the people and goods that are approaching our borders. One part of this mission is the capability to maintain and record the location and activities

of known and potential threats. This capability will enhance the likelihood of preventing attacks by providing the nation with an increased awareness of the actions of terrorists. With an infinite number of resources, the location of any and every conceivable threat might be maintained. Unfortunately, this goal is most likely unattainable. Therefore, efforts must be made to identify those threats that require the greatest attention.

The identification of a desired tracking capability will be largely dependent on the prioritization of recognized threats. Experts in the fields of border control and intelligence will be required to identify what threats need to be tracked the most. These SMEs can provide the knowledge necessary to define a target level of effort and a bare minimum list of threats that should be tracked. If the Federal government chose to ignore the activities of every threat, the nation would be severely at risk. Thus, efforts will always need to be made to maintain the location and activities of the most imminent threats.

Screening

Another component of the border awareness mission is the capability to observe, identify, and report information pertaining to people and goods attempting to gain access to the United States. If the appropriate agencies do not screen who and what enters the country, then the capability to deny access to terrorist threats will be significantly reduced. The security gained will be largely dependent on the intensity of the screening procedures that are imposed. On the other hand, excessive procedures may require an unacceptable number of resources and impede the travel of the innocent. Accordingly,

efforts should be made to enhance the speed and effectiveness of all screening procedures, while minimizing the associated costs. This ability to quickly access threat information at all borders and ports of entry is extremely reliant on enhancements in technology.

Experienced and knowledgeable SMEs will be required to clarify the desired levels of rapidity and effectiveness. The effort to avoid hindering the passage of legitimate travelers and shipments should not compromise the thoroughness of the screening process. Thus, the target level should balance these issues in an attainable manner. Similarly, because the United States cannot afford to open the nation's borders to anyone and anything, without attempting to identify if they are permitted to enter, a minimum capability to screen people and goods should be defined.

Inspecting

The final component of border awareness, defined in this study, is the capability to physically verify the security of the people and goods attempting to enter the country. The screening process attempts to identify who and what is a potential threat to the United States, while the inspection process is intended to verify whether the potential threat needs to be of concern. This process may include, but is not limited to, the physical inspection of shipping containers, passenger baggage, vehicles, and the travelers themselves. Just as with screening, this process needs to be as quick and effective as possible in order to steer clear of slowing the travel of legitimate traffic.

The target level for inspection capability will include many of the same concepts as screening. Speed, thoroughness, and accuracy must all be balanced in the definition of a desired level of capability. All potential threats, identified in the screening process, must be verified to be secure. However, it would be logistically infeasible to comprehensively inspect *every* person or good that approaches the nation's border. In contrast, if the United States chooses not to verify the security of anything, our nation would be in peril. Thus, the lowest acceptable capability in this area must be clearly delineated.

Control

A complete awareness of the people and goods approaching the nation's borders would be of limited utility without the capability to control who or what actually enters the country. The defensive capability to deny access to those people and goods that should not enter the United States is vital. Border control authorities must be able to apprehend individuals attempting to illegally enter the country; whether this occurs on land, sea, or air. Additionally, the U.S. military must gain and maintain the capability to defend the nation from the threat of ballistic missiles and other unmanned threats. Every effort should be made to prevent terrorists and their weapons from entering the United States and endangering the lives of its citizens.

However, it is also recognized that it would be virtually impossible to deny access to every conceivable threat. The effort to defend the nation's borders should be focused on those ports of entry that pose the *greatest* threat. Consequently, the target border

control capability, as defined by SMEs, must include some assessment of the risk involved with various defense strategies. Because the complete elimination of risk is not an attainable goal, the target capability will be required to clarify the level of risk reduction that is desired. At the same time, these SMEs must establish the highest level of risk that is acceptable; this defines the minimum capability.

Deterrence

In addition to denying the entry of recognized threats, the Federal government must take action to reduce the threat itself. The first component of threat reduction, as defined in this research, is the prevention from action by instilling fear of the consequences. Terrorists and terrorist groups must be made to believe that the United States has the capability and the intent to do what is necessary to secure the nation from terrorism. The effort to instill this belief will involve a variety of political and operational activities. The Departments of State, Defense, and Homeland Security will all play significant roles. The more potential terrorists the United States can deter from actually carrying out attacks, the more secure the nation will be.

A target level for the capability to deter terrorism will be difficult to define. Ideally, every potential terrorist would be prevented from even considering an attack within the United States. Unfortunately, the motivation of today's terrorists suggests that it may be virtually impossible to accomplish this. Thus, experienced and well-informed SMEs must be leveraged in the definition of a desired level of deterrence capability. One possibility might be to define a target audience that has the highest probability of being

influenced by deterrence efforts. Because some of today's terrorists cannot be deterred, it will be important to identify those who have the potential to be affected. Though it is a difficult mission area, the United States must not completely eliminate efforts at deterrence. If potential terrorists foresee no consequences for their actions, then they will be more likely to believe their attacks will go unpunished. Accordingly, some minimum level of deterrence capability must be defined.

Financial (Means Denial)

Beyond efforts to deter terrorist activity, the Federal government must take action to deny terrorists the means of attack. Every effort must be made to impede or prevent access to the financial support necessary to facilitate terrorist operations. By stopping the financial supporters of terrorism, the threat to America will be greatly reduced.

The SMEs in this area of expertise may very well ascertain that the target level is to achieve the capability to deny financial support to any and every terrorist and terrorist group that threaten the United States. On the other hand, this may be deemed logistically and operationally infeasible. The desired level of capability may be to eliminate the support to target groups. Al Queda, for example, may be the terrorist organization that the SMEs decide should be targeted for means denial. In this case, the desired level might be to have the capability to deny 100% of the funds that support al Queda. In stark contrast, the targeting of a single group may be defined as the minimum acceptable capability. Here, SMEs may determine that the target level is to have the capability to

deny the funds of multiple groups. Regardless, it will be up to the experts in the field to establish the minimum requirements and target capabilities in this area.

Logistical (Means Denial)

The second form of means denial that the Federal government must have the capability to execute involves logistics. In particular, terrorists must be prevented from obtaining the weapons and delivery systems that could be utilized in an attack on America. It is recognized that it is virtually impossible to deny terrorists access to every type of weapon and that new means of attack will always be discovered. However, every effort must be made to prevent terrorists from acquiring the world's deadliest weapons; namely chemical, biological, radiological, and nuclear weapons.

The driving factor in defining a target capability in this area will likely be the determination of which weapon systems to attempt to deny access to terrorists. Though it is no doubt desirable to have the capability to prevent terrorists from accessing every conceivable weapon, this goal is not attainable. SMEs will therefore need to define what weapon systems the Federal government should pursue securing. Perhaps the target level would be to have the capability to deny terrorists access to weapons of mass destruction. Much like financial means denial, however, it may be determined that this capability is only a minimum. In this case, the target capability might include preventing terrorists from acquiring any form of explosive material as well as the technology required to launch cyber attacks. The expertise of the appropriate SMEs will be needed to establish what weapon systems should be targeted.

Law Enforcement

In addition to denying terrorists the means of attack, efforts must be made to target terrorists themselves, as well as their supporters. These efforts will be both preemptive and retaliatory. However, regardless of the chronology of the actions taken, the true value of these efforts is their ability to *prevent* terrorists from executing future attacks. Law enforcement will play a major role in reducing the threat of terrorism by tracking down, arresting, and prosecuting those who commit terrorist acts, or support such acts. Because it is vital that terrorists are brought to justice, police officers and judicial personnel must be given the proper training to deal with the unique nature of prosecuting terrorism. Valuable evidence must be obtained and utilized in the court of law in a manner that facilitates convictions. These activities will be paramount in the effort to prevent future terrorist attacks.

SMEs experienced in the law enforcement community will be needed to define the most desirable level of capability in this area. Again, in an ideal world, every future terrorist would be hindered from carrying out attacks. Unfortunately, it may prove extremely difficult to convict every potential terrorist before they can execute an attack. In the face of this difficulty, the Federal government must ensure that the United States has the necessary numbers of trained individuals to combat the terrorist threat. Accordingly, the desired level of capability in this area may involve the definition of a target law enforcement workforce (i.e. number of personnel). On the other hand, a larger workforce will provide little benefit if they are not properly trained. Thus, a target level

for training will likely be needed. It will also be necessary to define the minimum law enforcement workforce required to combat terrorism within the United States.

Military

The effort to deny the actions of terrorists will necessitate the support of the nation's military. The operations in Afghanistan, following the attacks on 9/11, demonstrate the role that the military must play in reducing the terrorist threat. The annihilation of terrorist training camps and the disruption of the command and control of terrorist organizations are vital. The Federal government must utilize all of its assets, including the military, to bring terrorists to justice.

Just as with law enforcement, military experts must be leveraged in the effort to define a target capability. Military personnel must be trained in anti-terrorism and counter-terrorism tactics and must be properly equipped to perform their mission. The appropriate SMEs must define the content and intensity of this training as well as the number of personnel to be trained. The target level should capture all of the aspects necessary to clarify exactly what military capability the United States should pursue in order to prevent terrorism. Similarly, the minimum requirement will likely include some elaboration into the smallest military unit that should be maintained as the nation's terrorism combat force. A minimum number of personnel and training must be defined.

Other

The final category of action denial, defined in this study, includes those remaining authorized agencies and organizations that may target terrorists and their supporters. While law enforcement and the military will likely play the most significant roles, the covert and clandestine communities may also execute an array of responsibilities.

The definition of capabilities in this area will be extremely reliant on the specific knowledge of experts in the field. A target level may prove quite pervasive. Then again, these agencies and organizations will *also* be required to train, exercise, and equip an array of personnel, much like law enforcement and the military. The target and minimum acceptable capabilities, therefore, may include the same considerations as these. The Federal government must foster the specialized capabilities of the intelligence community as one more means of denying the actions of terrorists.

Vulnerability Reduction Measures

This section delineates the topics and issues that might be considered when developing the capability continuums for the six critical objectives depicted in the *Vulnerability Reduction* branch of the hierarchy in Figure D-1.

Identification

As the initial component of assessing the nation's critical infrastructure and key assets, it is paramount that the Federal government has the capability to determine which

people, systems, symbols, facilities, functions, and events are critical to national security, governance, public health and safety, economy, and morale. Rather than exhausting vital resources attempting to hypothesize what terrorists intend to target, more benefit is provided by the identification of which targets will have the greatest impact. Accordingly, the continuous recognition of those infrastructures and assets that are most critical to the United States is a valuable mission in the effort to reduce America's vulnerabilities.

The efforts of the PCCIP and various other critical infrastructure studies have demonstrated that the United States does have a great deal of capability in this area. Those infrastructures that are most critical have been listed in numerous pieces of literature. At the same time, however, the nation's critical infrastructures are fluid. What is critical today, may be of less significance tomorrow. Though SMEs have identified our *current* critical infrastructures, a potential target level is the capability to perform this identification continuously. The Federal government may deem it desirable to pursue the near real-time determination of what is critical. This capability would provide the United States with the necessary information to maintain an *accurate* assessment. If continuous identification were determined to be the target level, then the minimum requirement would likely be some wide interval of time. The clarification of this time interval would require the support of the appropriate SMEs.

Analysis

Once the nation's critical infrastructures have been identified, they must be reviewed and evaluated to determine those areas that are most at risk. This analysis will include the mapping of recognized threats against current vulnerabilities. The integration of terrorist threats and critical infrastructure vulnerabilities is a necessary step if a true understanding of risk is to be developed. The Federal government will require not only experienced personnel, but also the associated technological capabilities in order to accomplish this mission.

The definition of a target capability to analyze the nation's critical infrastructures will likely be driven by the need for a rapid and continuous understanding of what is at risk. Current threats must be quickly compared to existing vulnerabilities in order to identify those infrastructures that are in the most imminent danger and to implement protective action. As with the determination of what is critical, this must be performed continuously. Thus, the target level must address the desired time horizon for analysis. Additionally, a minimum time interval for the results of this analysis must be determined in order to ensure that the United States has some acceptable level of capability. The analysis of America's critical infrastructures and key assets is a precursor to their prioritization to determine what should be protected first.

Prioritization

Because it is fiscally, logistically, and operationally impossible to protect every potential terrorist target, the Federal government must establish some priority for the

allocation of effort and resources. The analysis process is performed to ascertain which infrastructures and assets are most at risk. Based on that analysis, the appropriate decision-makers must determine where to apply protective resources. Because homeland security is such a dynamic mission area, this decision process must be conducted on a continuous basis. Threats and vulnerabilities change; so too should the prioritization of protection.

Just as with the entire assessment process, SMEs will likely determine that the desired level of capability to prioritize our critical infrastructures is largely dependent on time. America's critical infrastructures must be identified, analyzed, and prioritized as swiftly as possible, and on a constant basis. Consequently, the target level should reflect the speed and update interval specified by well-informed SMEs. If the Federal government had no capability to prioritize the nations vital infrastructures and assets, then a large number of resources could be squandered attempting to protect a target of little consequence. Because of this, some lowest level of prioritization capability should be determined.

Vigilance

Once it has been determined which critical infrastructures and key assets require the most imminent defense, protective measures must be implemented. One component of this effort is to increase the awareness and watchfulness of the sectors and populations at risk. The Federal government must have the capability to warn the nation of potential threats and the vulnerabilities that those threats intend to exploit. Well-informed

warnings must reach as much of the target audience as possible and do so in a rapid manner. An array of systems, including the Homeland Security Advisory System, will need to be employed to accomplish this.

The question of how big an audience to target must be addressed by the appropriate SMEs. Ideally, every individual or infrastructure that is determined to be at risk could be warned early enough to facilitate protection. At the same time, the Federal government must guard against disseminating warning information too frequently, lest the nation become desensitized. The target level must address the need to reach target audiences quickly, yet only when the threat information has been appropriately confirmed. In contrast, at a minimum, critical infrastructure sectors and American citizens must be warned when the threat is *imminent*. The minimum acceptable level of capability must establish the smallest target audience and minimum lead-time necessary to ensure that adequate defenses can be implemented.

Readiness

The second form of protection recognized in this study is the establishment of contingency plans, policies, and standards. These activities are performed in order to ensure the ability of critical infrastructure sectors to deliver the key services for which they were designed. In the face of a potential attack, the nation's vital systems and services must be prepared to persevere. This will be accomplished through planning, training, and exercising the personnel and systems that are responsible for administering critical infrastructure services.

A target level of readiness may be difficult to define. The intensity of the preparedness will likely be driven by the enormity of the threat. Accordingly, various infrastructure sectors may require dissimilar levels of readiness. SMEs in each sector will be able to provide the insight necessary to define target planning, training, and exercise capabilities specific to their sector. Additionally, the establishment of the desired capability might consider the level of readiness with respect to various threats. While it is beneficial to be prepared for one form of attack, it is of even greater value for critical infrastructure sectors to be prepared for an array of attacks. Robust approaches may well be preferred. A minimum level of readiness may be equally difficult to define. Some form of contingency planning must take place in each sector. The comprehensiveness of that planning, however, must be defined by the appropriate SMEs.

Surety

The final form of protection involves physical and cyber measures designed to prevent unauthorized access to critical infrastructure and key assets, and to safeguard them against loss or damage. In contrast to the previous two capabilities (vigilance and readiness), this concept accounts for more recognizable forms of protection. Physically hardening a facility, implementing computer firewalls, administering inoculations and maintaining a reserve of personnel to respond to a surge of demand are all actions taken to increase surety.

Much like readiness, the intensity of efforts to physically ensure a particular infrastructure will likely be dependent on the threat to that particular sector. Thus, the

target level of capability must capture the needs of each sector. At the Federal level, SMEs may ascertain that the target capability should be to physically protect as many infrastructure sectors as possible. Though dissimilar sectors may not require the same level of surety, the target would be to provide each sector with the protection it requires. At a minimum, the Federal government must have the capability to ensure that each sector has some semblance of surety. Accordingly, the minimum required capability must capture the bare minimum needs of each sector.

Response Preparedness Measures

This section delineates the topics and issues that might be considered when developing the capability continuums for the ten critical objectives depicted in the *Response Preparedness* branch of the hierarchy in Figure D-1. For these objectives, it makes sense to measure the impact on the nation's capability with respect to the attack methods that terrorists can employ. Because the objectives included in this branch of the larger hierarchy are designed to address an attack that has already occurred, they must speak to an array of weapons. Terrorists and terrorist groups "are working to obtain chemical, biological, radiological, and nuclear weapons for the stated purpose of killing vast numbers of Americans" (National Strategy, 2002:9). In addition to weapons of mass destruction, terrorists continue to utilize conventional weapons, such as bombs and guns, and seek new ways to magnify their effects (National Strategy, 2002:9, McIntyre, 2002:np). Finally, the pervasiveness of computer expertise has established cyber attacks as another significant threat (National Strategy, 2002:9, McIntyre, 2002:np). These six

methods of attack (chemical, biological, radiological, nuclear, conventional, and cyber), arrayed against response preparedness objectives, produce mission areas that the United States must have the capability to execute in order to minimize the damage and recover from terrorist attacks. Accordingly, the capabilities described below are intended to address each of these six methods individually.

Attack Detection

The capability to identify, recognize, confirm, and report the occurrence of a terrorist attack within the United States is vital. If an attack is not detected in a timely manner, then it will prove difficult to deploy an effective response. Immediately after an attack occurs it must realized, classified (i.e. what type of attack), comprehensively confirmed and then reported to the appropriate audience; including the American public. If the affected population is not alerted quickly, the chance of mitigating the effects of the attack is severely reduced.

Clearly, in this case, the target capability will be greatly dependent on the time to detection. The ideal case would be to detect all forms of attack *immediately*. Unfortunately, some types of attack, such as biological and cyber, can be difficult to identify until they have already taken affect. Because of this, the appropriate SMEs must establish target detection times for each form of attack. The technology required to accomplish detection will be equally dependent on the type of attack. The target capability must therefore address the technology necessary to achieve the desired level of detection. In contrast, the nation must maintain some minimum capability to detect

attacks in order to facilitate a response. The minimum acceptable time horizon to detect an attack will be specific to the means of attack and must allow for some form of response, at the very least.

Rapid Response

Once an attack has been recognized and reported it will be necessary to quickly assess the extent of the attack, recommend response options, and deploy response teams. The rapidity of the response will be dependent on an array of factors. The means of attack will be a significant factor, however, the population density and relative significance of the target area are also major consideration in the development of a response plan. The time interval between the report of an attack and the arrival of response teams on-site should be as small as is required to effectively mitigate the incident.

Much like detection, therefore, the target deployment capability will likely be defined with respect to time. In general, faster response times will be preferred. On the other hand, the definition of "fast" will be driven by the potential effects of the attack in question. Issues such as political sensitivity must be addressed hand in hand with the training and equipment necessary to effectively deploy a response. The establishment of a minimum acceptable capability will be equally fraught with political, logistical, and operational considerations. At the very least, response teams must have the capability to deploy to an attack site quickly enough to save the life and limb of those directly affected.

Treatment

When they have arrived on-site, response teams must be capable of administering the level of care necessary to save life and limb and stabilize victims sufficiently to withstand evacuation to the next level of care. The variety of injuries that could potentially be incurred from terrorism is as pervasive as the methods of attack. Consequently, emergency health care providers must be properly trained, exercised and equipped to address a wide array of contingencies. The immediate effects of a biological attack may require a different response than the initial treatment required by the detonation of a nuclear weapon. Dissimilar attacks will require a variety of treatments. Regardless, response teams must have the capability to save as many lives as possible.

Emergency response SMEs would provide the most beneficial body of knowledge in the effort to define a desired level of capability to treat the victims of terrorist attacks. An obvious target level would be the capability to save the life of *every* individual affected by a terrorist incident. However, in the wake of a nuclear detonation, for example, the number of people immediately killed, before a response team can even arrive, will make this goal unattainable. The target level of lives saved, therefore, will be extremely dependent on the means of attack. Subject to the insight of the appropriate SMEs, the minimum requirement might be to ensure the successful treatment of all those who are alive upon the arrival of the response team. This would account for the immediate impacts of differing forms of attack.

Containment

In order to prevent the spread of the effects of a terrorist incident, response teams must have the capability to stop, hold, or surround an attack. The comprehensiveness of this containment will be largely dependent on the method that terrorists choose to employ. While a biological attack might potentially be contained through quarantine, the radiation and fallout that results from a nuclear detonation is at the mercy of the environment. While a cyber attack may be able to spread at the speed of light, it might be stopped and its effects held within a certain network. A chemical attack, on the other hand, would spread as quickly as the wind blows. Thus, the capability to contain various attacks will require a broad spectrum of training and equipment.

There is no doubt that it would be desirable to stop an attack before it could have any material effects. In addition, the benefits gained by quickly concentrating the effects of an attack that cannot be stopped are obvious. At the same time, *speed* is not the only factor that should be considered when defining a target capability. The containment must be *comprehensive* enough to eliminate the possibility of the attack spreading for use elsewhere. It would also be preferred to implement this containment in as little a radius as possible. The target radius, however, will depend on the extent of the original attack area. At the very least, the effects of the attack must be slowed or contained to a greater extent than would have occurred if no response had been implemented. The establishment of any minimum requirement beyond this will necessitate the insight of SMEs.

Decontamination

The immediate effort to minimize the damage of terrorist attacks must be complemented by long-term activities that facilitate the eventual recovery of the nation. One portion of this objective is the capability to absorb, destroy, neutralize, make harmless, or remove the effects of an attack. Because the United States is extremely reliant on the systems and facilities that may be potentially affected by an attack, it is paramount that contaminated areas are made safe for use as quickly as possible. Furthermore, it is vital that the decontamination process is performed thoroughly and accurately to ensure that no side effects occur once the systems and facilities have returned to operations.

In some cases, the need for thoroughness may outweigh the need for a speedy return to service. The Anthrax attacks following 9/11 proved that workplaces and public facilities must be comprehensively decontaminated in order to instill confidence that the affected area is safe. Accordingly, the target capability in this area will likely focus on the reliability of the process as much as the speed with which it is implemented. It is recognized that the effects of an attack must be removed quickly; however, a speedy, *unreliable* exertion of resources is of little worth. The effects of an attack must eventually be completely, reliably removed. Thus, as a minimum requirement, the appropriate entities must be capable of decontaminating the attack site in some finite period of time. The quicker they are capable of accomplishing this, the closer they will be to achieving the target level.

Restoration

To further the recovery process, the United States' critical infrastructures and key assets must have the ability to reestablish operational capabilities. Any break in the services provided by these vital systems must be as inconsequential as possible. Because the nation's critical infrastructures are such viable targets, they must be prepared to address the consequences of an attack. The cyber-based linkage between many infrastructure sectors suggests that an attack on a single target could potentially cascade across numerous sectors. It is, therefore, vital that each sector has the capability to restore the services it was designed to provide. The speed and extent of this restoration will depend largely on the impact of the attack and the sector in question.

The establishment of a target time horizon for restoring the services provided by America's critical infrastructures will require the expert knowledge of infrastructure owners and operators. Additionally, the target level for the restoration of services destroyed by a small-scale explosion may differ significantly from the target associated with a nuclear explosion. Clearly, the means of attack must be taken into consideration in defining desired levels of capability. The minimum acceptable level of capability in this area will likely be difficult to specify. All things being equal, the nation's citizenry is probably capable of surviving longer without electricity than without food and water, for example. Varying infrastructure sectors will require specific definitions of minimum requirements and a clear understanding of the repercussions of these requirements.

Reconstruction

Merely reestablishing the operational capabilities of the systems and services affected by an attack is fundamentally different from returning the item to a standard as nearly as possible to its original condition in appearance, performance, and life expectancy. Reconstruction applies not only to the act of physically rebuilding facilities, but also to *completely* restoring the critical infrastructures affected by an attack. While restoration accounts for the sheer ability to provide the service, in any form, reconstruction applies to the ability to return the target to its original condition. This does not necessarily have to occur at the original attack site. The World Trade Center towers, for example, may never be rebuilt, but the services provided there could be completely restored at other locations. This would still constitute reconstruction.

The desired level of capability, in terms of speed and extent, to rebuild the targets of terrorist attack, will likely be dependent on the significance of the target. The reconstruction of a scarcely used bridge may not require as imminent an effort as the wall of the Pentagon required after 9/11. The desired speed for reconstruction, as well as the extent, will be driven by the importance and significance of the services provided by the target. While the time horizon for one reconstruction project may be defined in days, another may be defined in years. It will be up to the appropriate SMEs to determine these targets as well as the minimum acceptable levels of reconstruction.

Medical (Assistance)

The disastrous effects of terrorism suggest that the capability to provide an array of long-term assistance to victims is critical. One of the *most* critical forms of aid is long-term medical care. In contrast to the *Treatment* value discussed earlier, this value captures the capability to administer care beyond efforts to immediately save life and limb. Ongoing treatment as a result of exposure to radiation or toxic chemicals, as well as psychological counseling to deal with the emotional trauma associated with terrorist attacks would be accounted for here. The Federal government must make every effort to assist and support all of the victims of terrorism.

In an ideal world, every single victim that requested long-term medical care would be provided with it. Limited resources may, however, deem this infeasible. Accordingly, the target capability in this area may be the provision of long-term medical treatment to all those who *require* it, rather than all those who request it. The capability merely to provide assistance as necessary and required could potentially be a daunting task in itself. At the same time, this target capability would likely still be attainable. At the very least, long-term medical care must be provided to those who would perish without it. The establishment of minimum requirements above and beyond this capability would require SME support.

Financial (Assistance)

In addition to long-term medical care, the Federal government must have the capability to provide financial assistance to those victims who are fiscally impacted by

the consequences of terrorist attacks. The attacks on 9/11 demonstrated that the effects of terrorism include unemployment, loss of property, and the death of families' primary source of income. The victims of such effects may be left without a home or the ability to provide for their family. Consequently, it may be required to provide cash grants, low-interest loans, unemployment benefits, free legal counseling, and tax refunds (National Strategy, 2002:45).

The extent of this support will likely be dependent on the resource and budgetary constraints of the entities providing assistance. Because of this, the *complete* provision of financial assistance to all who request it may not be an attainable goal. A more sensible target level might be the capability to provide fiscal support to all those who absolutely require it. Much like medical assistance, well-informed SMEs will be needed to establish the target audience for financial support. The same experts will be needed to define the absolute minimum audience that should be provided with assistance.

Logistical (Assistance)

The final form of assistance to victims, considered in this study, is the provision of logistical support. This value accounts for the array of additional forms of assistance, above and beyond medical and financial, that the Federal government must have the capability to provide. In the face of a terrorist attack, victims may require transport, temporary living facilities, food and water, clothing, and an organized system to communicate their concerns. Just as with any humanitarian operation, the logistical aspect of assisting victims is critical.

The target capability to provide logistical support will likely be no different than the previous two forms of assistance. Scarce resources must be applied to those victims who need it most. In an ideal world, every single victim would be provided with the support that they request. In some cases, subject to the extent of the attack, this may be attainable. On the other hand, the most catastrophic attacks will likely overwhelm the services attempting to provide assistance. In this case, the target capability must consider the availability of logistical resources. Again, as a bare minimum, assistance must be provided to those victims who would perish without it.

Appendix E: Resource Costs and Civil Liberties Measures

This appendix provides a more detailed elaboration of the measures and single dimension value functions utilized to assess the attainment of the considerations included in the Resource Costs and Civil Liberties hierarchies.

Consideration of Resource Costs

Figure E-1 displays the Resource Costs hierarchy presented in Chapter 4. The measures developed in this research are also included.

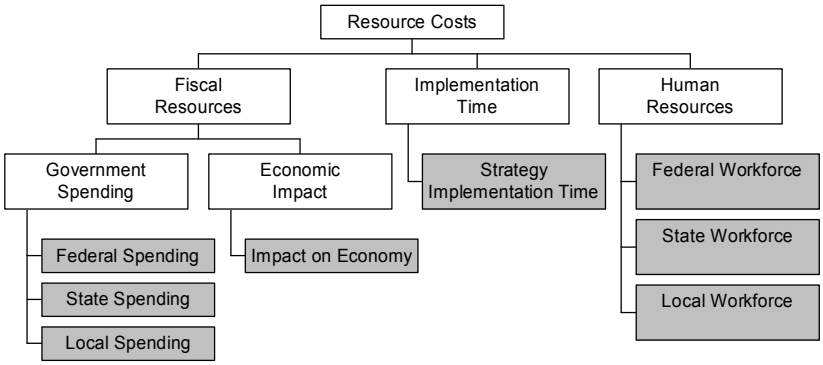

Figure E-1: Resource Costs Hierarchy with Measures

These measures are described in more detail below, along with the single dimension value functions (SDVFs).

Fiscal Resources (Federal, State, and Local Spending)

The scope of this research dictates that budgetary spending at the federal level of government should be considered in the development of homeland security strategy.

However, because decreases in federal spending on federal mandates can potentially lead to increased state and local spending to ensure the execution of strategy, this research considers homeland security spending at all levels of government. Given a proposed strategy, each level of government may be required to allocate a portion of its budget to support implementation. Because the implementation of a particular strategy could take multiple years, this allocation of fiscal resources might fluctuate from one fiscal year to the next. However, this fluctuation can be overcome and the total cost can be calculated using net-present value (NPV). The value achieved by this cost will be dependent on the level of government in question.

It is assumed that lower costs are preferred at all levels of government, however the upper bounds on spending are defined by the constraints of the individual budgets under consideration. What is considered a significant cost at the state or local level may not necessarily be significant at the federal level. As was described in Section 4.3.1. it is projected that the Federal government will spend $37.7 billion in FY2003, while state and local governments are projected to spend as much as $5.1 and $13.9 billion respectively (Deloitte Consulting, 2002:1). Though this is the projected *overall* spending on homeland security solutions, it provides insight as to the relative significance of spending on *individual* solutions (i.e. strategies). According to these projections, State governments will spend 14% of what the Federal government spends and local governments will spend 37%. If it is assumed that $1 billion (in NPV) is the least preferred level of spending on a single strategy at the federal level, then, using these percentages, the least preferred levels for state and local spending are $140 million and

$370 million respectively. Given these assumptions, the SDVFs displayed in Figures E-2 through E-4 are used to assess spending for federal, state, and local governments.

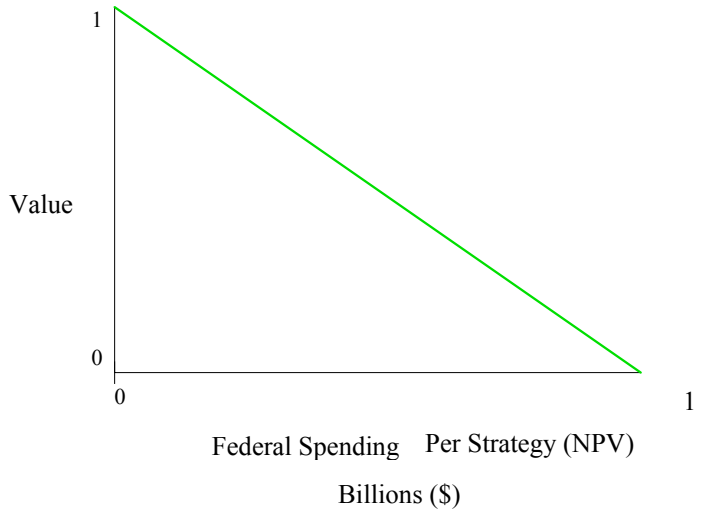

Figure E-2: SDVF for Federal Spending

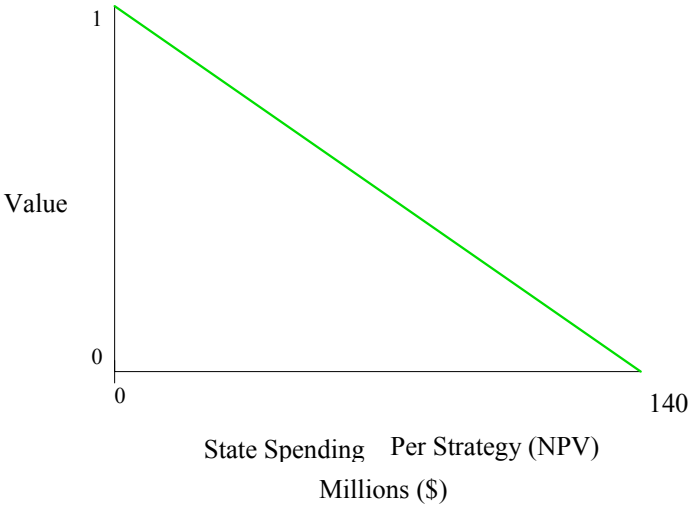

Figure E-3: SDVF for State Spending

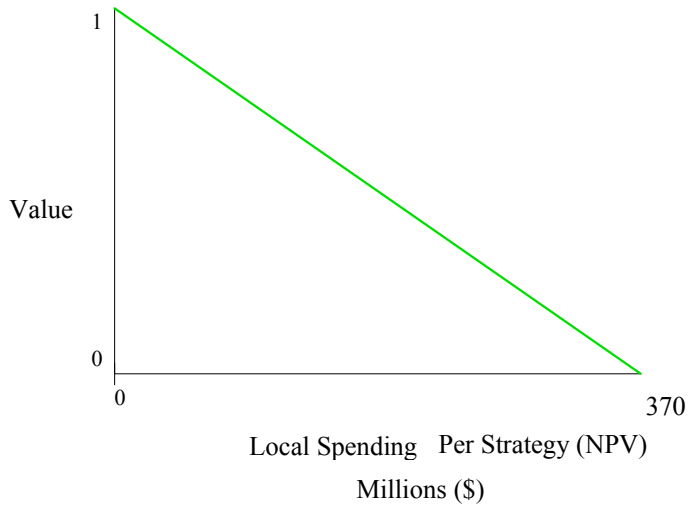

Figure E-4: SDVF for Local Spending

Thus, the maximum value, in terms of fiscal resources, is attained by **a** strategy that requires no budgetary spending. Alternatively, a strategy that consumes the maximum acceptable amount (or more) defined for the budget of interest receives zero value.

Fiscal Resources (Impact on Economy)

Efforts to enhance security will reduce the risk to which the American people are currently exposed. However, these efforts may potentially impact the United States economy because of their capability to reduce the desire of the American people to spend money. The events of 9/11 scared many citizens to the point that they refused to travel by air. Furthermore, the airline industry might suffer, financially, if airport security measures continue to require drastic increases in time delays. The preference for air travel as a rapid means to reach a variety of destinations may soon diminish if passengers

are required to check-in at earlier and earlier times. The example of the airline industry demonstrates how increased security could negatively impact an array of public services, and thus the U.S. economy.

The value provided by a particular strategy will be dependent on its perceived impact on the U.S. economy as a whole. Obviously, the preference is that it has no negative impact at all. In this case, the economic prosperity of the nation would continue on untarnished. In contrast, if it is determined that a strategy *will* negatively impact the economy, the greater impact it has, the less valuable it becomes. This determination will be greatly dependent on the expert knowledge and input of a variety of high-level decision-makers. The SDVF in Figure E-5 is used to assess the impact on the United States economy.

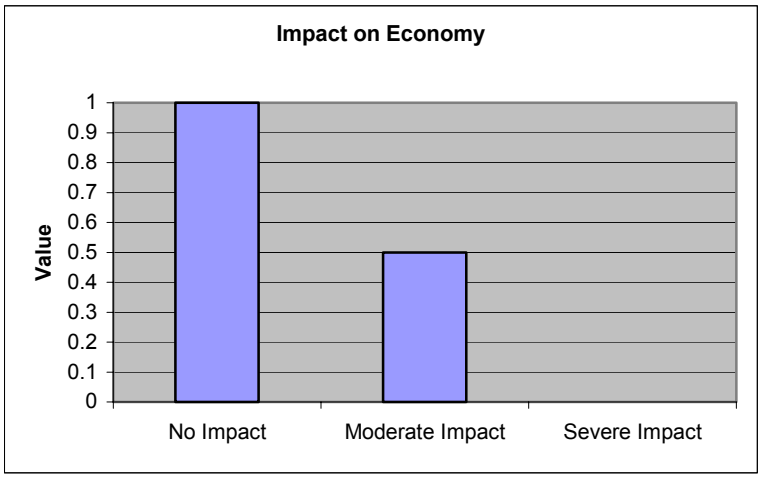

Figure E-5: SDVF for Impact on Economy

The clarification of exactly what can be considered a moderate or severe impact will be dependent on the insight of the appropriate subject matter experts. In general, however,

the greater an impact a strategy has, the less value it achieves. While not incorporated in this study, a measure for positive economic impact could easily be implemented.

Implementation Time (Strategy Implementation Time)

As was acknowledged in the previous section, dissimilar strategies could require disparate lengths of time to implement. While the research and development of a new version of a detection tool might require 1-2 years, the organization and activation of an entire new agency or department might require 5-10 years to fully implement. Though it is recognized that strategies with faster implementation times are not always superior, in general the longer it takes to fully implement a strategy the longer the United States remains insecure. Therefore, in measuring the time required to fully implement a particular strategy, this research assumes that quicker times are preferred. The security provided by the strategy is measured in the Homeland Security hierarchy.

The upper bound for implementation time is defined as 20 years. It is assumed that a strategy that requires more than 20 years to implement will be ineffective in the immediate future in securing the homeland in an acceptable amount of time, and thus receives zero value for the Implementation Time measure. Additionally, implementation times of five years and less receive high value, while times beyond five years lose value quickly. This behavior is supported by the estimated time required to fully establish the Department of Homeland Security (roughly five years or less) and the perceived value obtained by this strategy. The SDVF in Figure E-6 accounts for the desired behavior.

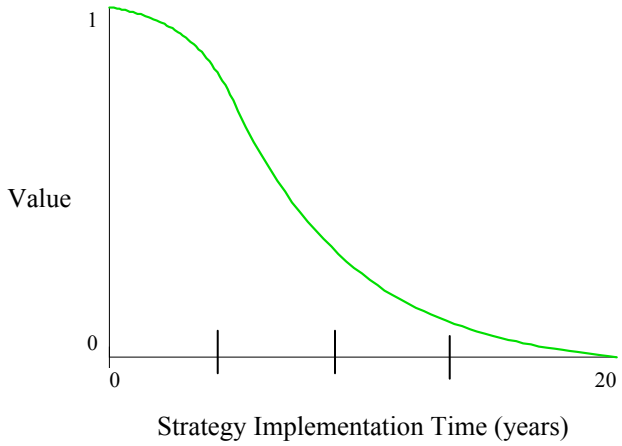

Figure E-6: SDVF for Implementation Time

The maximum value is attained by a strategy that can be fully implemented immediately, whereas a strategy that requires 20 years or more provides zero value. As desired, the value associated with a particular strategy drops off dramatically after five years.

Human Resources (Federal, State, and Local workforces)

The final resource cost measured in this thesis addresses the personnel required to implement the strategy of interest. As with fiscal resources, changes in the homeland security workforce will occur at the federal, state, and local level. It is assumed that all levels of government prefer the minimization of increases in personnel. This is due to the acquisition, relocation, and training required when a workforce is increased. Additionally, it is assumed that the percentage increase in personnel captures the difficulties associated with these requirements. Finally, because certain strategies might

require the workforce to more than double (i.e. more than 100% increase), it is assumed that any increase more than 100% of the current level receives zero value.

It is recognized that the original size of the workforce in question will be dependent on the level of government and the associated organization. However, the use of percentages accounts for variations in the original size of the workforce. This research uses the SDVF in Figure E-7 to measure the impact on workforces at the federal, state, and local level (one function for each).

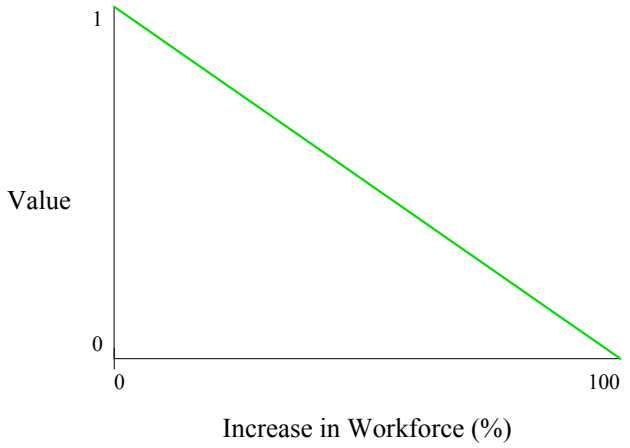

Figure E-7: SDVF for Increase in Workforce

The maximum possible value, in terms of human resources, is attained by a strategy that can be implemented with the current workforce or less (i.e. zero increase). If a particular strategy dictates that the workforce more than double, then zero value is provided.

Consideration of Civil Liberties

Figure E-8 displays the Civil Liberties hierarchy presented in Chapter 4. The measures developed for this hierarchy are included here.

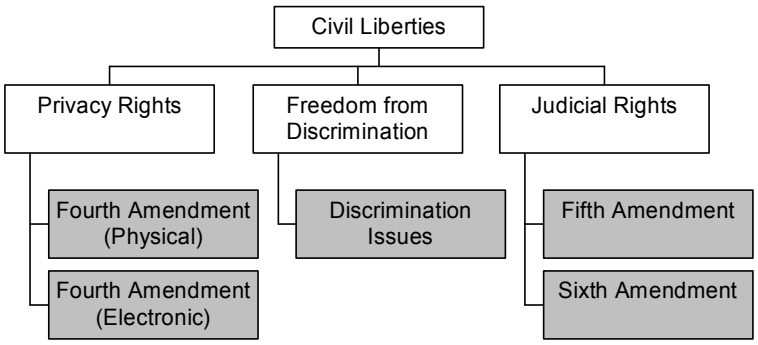

Figure E-8: Civil Liberties Hierarchy with Measures

These measures are described in more detail below, along with the single dimension value functions (SDVFs).

Privacy Rights (Fourth Amendment)

As recognized by Privacy International and the Electronic Privacy Information Center, the U.S. Constitution contains no explicit right to privacy. However, the Supreme Court has ruled that the Bill of Rights, in particular the Fourth Amendment, does contain a number of provisions that offer a limited constitutional right to privacy. Thus, the Federal government must be concerned with the impact that efforts to prevent terrorism have on the privacy of innocent Americans. This research assesses whether or not a particular strategy has the **potential** to impact the provisions of the Fourth Amendment as a proxy for measuring the impact on privacy. Because this research

addresses the homeland security problem at the highest levels of government, it is appropriate to measure the impact on privacy rights at the highest levels of responsibility. The Bill of Rights dictates the fundamental rights promised to all Americans. It is the responsibility of the Federal government to ensure these rights are not at risk.

The Fourth Amendment dictates that individuals have the right "to be secure in their persons, houses, papers, and effects" (Constitutional, 2003:np). The right to privacy in these four areas has the potential to be impacted by both *physical* and *electronic* searches and seizures. The increased security at the nation's airports, including searches of passengers and their baggage, provides one example of physical activities. The methods and means to be employed by the TIA (described in Section 4.5.1.) exemplify electronic actions. While physical searches will likely be performed in the open and known by the individuals being searched, electronic forms of surveillance may take place out of sight and unknown to anyone. Whether the activities are physical or electronic, the more areas (i.e. person, house, papers, and effects) they have the potential to impact, the less valuable the activities become. The SDVF in Figure E-9 is used for both physical and electronic activities (one for each) to evaluate whether any of the activities associated with a particular strategy have the potential to impact the provisions of the Fourth Amendment. It should be recalled, however, that the weighting process would capture whether the decision-makers feel that one type of search (physical versus electronic) is less preferred than the other.

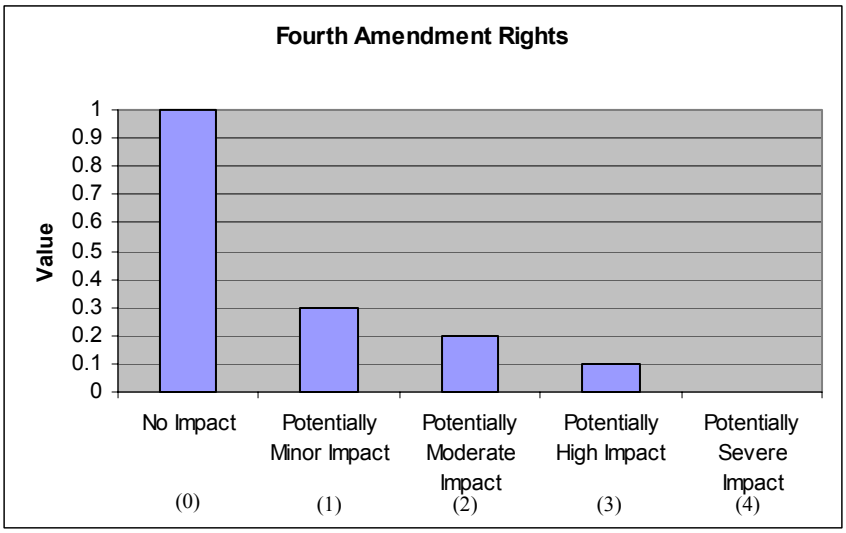

Figure E-9: SDVF for Fourth Amendment (Physical/Electronic)

What is considered minor, moderate, high, and severe, in this research, is presented in Table E-1. These definitions apply to both of the measures; addressing physical and electronic activities.

Table E-1: Definitions for Fourth Amendment SDVFs

Potential Impact?	Definition
No Impact	None of the physical/electronic activities associated the proposed strategy have the potential to impact the privacy of people's persons, houses, papers or effects.
Potentially Minor Impact	Potential impact exists in **one** of the following areas of privacy: persons, houses, papers, or effects.
Potentially Moderate Impact	Potential impact exist in **two** of the following areas of privacy: persons, houses, papers, or effects.
Potentially High Impact	Potential impact exist in **three** of the following areas of privacy: persons, houses, papers, or effects.
Potentially Severe Impact	Potential impact exists with **four** of the following areas of privacy: persons, houses, papers, or effects.

Obviously, the preference is that no portion of the strategy in question presents potential issues with the Fourth Amendment rights of any American. On the other hand, it is

recognized that the critical need to obtain information about potential terrorists may present issues with these rights. The more a strategy impacts the privacy of individuals in their persons, houses, papers, and effects, the less valuable it will be to homeland security decision-makers.

Freedom from Discrimination (Discrimination Issues)

It is vital that the Federal government make every effort to track down the individuals responsible for acts of terrorism within the United States and bring them to justice. However, in some cases, particularly when the suspected terrorists are believed to be from a specific ethnic or religious group, the nation's response has the potential to aggravate existing prejudices worldwide. Additionally, all response entities must be careful to avoid profiling suspects based on their cultural beliefs or origins. Thus, a method is needed to assess the discriminatory impact made by alternative homeland security strategies.

The Human Rights and Equal Opportunity Commission (HREOC) states that it is against the law to discriminate against individuals because of the following attributes: age, illness or injury, marital status, sex, physical features, political belief or activity, race, religious belief or activity, lawful sexual activity, pregnancy, status as a parent or carer, industrial activity or personal association. (HREOC, 2003:np).

Though discrimination should be equally circumvented in each of these areas, it is not likely that homeland security strategies would implicate prejudices in all of these areas. For the purposes of this research, sex, physical appearance, political belief, race or

ethnicity, religious belief, and personal association will be considered as areas of discrimination that may be potentially impacted by proposed strategies. The intent is *not* to downplay the importance of the remaining topic areas, but merely to recognize those areas that may present issues in the homeland security context. The SDVF in Figure E-10 is utilized in this research to assess whether any portion of a proposed strategy has the potential to raise discrimination issues in the six areas of impact chosen above.

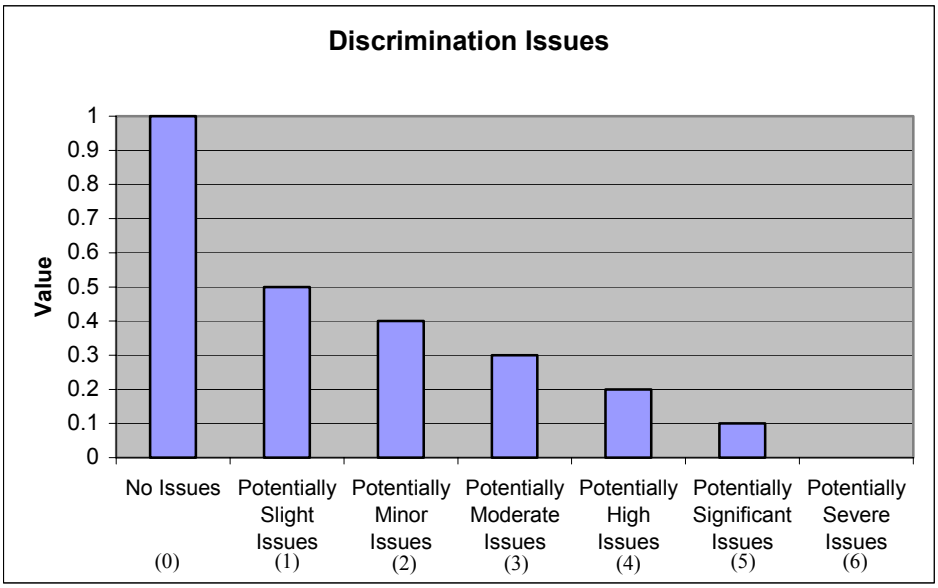

Figure E-10: SDVF for Discrimination Issues

Just as with the categories in the Fourth Amendment SDVF, what is considered Slight, Minor, and so forth, in this research, is defined in Table E-2.

Table E-2: Definitions for Discrimination SDVF

Potential Issues?	Definition
No Issues	None of the activities associated with the proposed strategy present discrimination issues with the following six characteristics: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.
Potentially Slight Issues	Potential issues exist with **one** of the following areas of discrimination: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.
Potentially Minor Issues	Potential issues exist with **two** of the following areas of discrimination: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.
Potentially Moderate Issues	Potential issues exist with **three** of the following areas of discrimination: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.
Potentially High Issues	Potential issues exist with **four** of the following areas of discrimination: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.
Potentially Significant Issues	Potential issues exist with **five** of the following areas of discrimination: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.
Potentially Severe Issues	Potential issues exist with **six** of the following areas of discrimination: sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association.

The decision-maker's preference would be to avoid any sort of discrimination issues in employing a new homeland security strategy. For this study, if a strategy avoids any discrimination issues, then the alternative achieves the highest value. Alternatively, the more a strategy may raise discrimination issues according to sex, physical appearance, political belief, race or ethnicity, religious belief, and personal association, the less valuable it becomes.

Judicial Rights (Fifth and Sixth Amendment)

The indefinite detentions and denial of access to legal representation of a number of suspected terrorists since 9/11 have raised concern over the judicial rights promised by

the Constitution. Much like the privacy rights discussed above, the Federal government must ensure that the fundamental rights to counsel and a fair trial are not denied to those who are entitled them. As part of this process, it is vital that the suspects are properly classified (e.g. material witness vs. visa violator vs. enemy combatant) to determine exactly what rights they are entitled.

This research assesses whether or not a particular strategy has the potential to impact the provisions of the Fifth and Sixth Amendments as a proxy for the affect on judicial rights. The Fifth Amendment addresses the rights promised an individual being charged with a "capital, or otherwise infamous crime" (Constitutional, 2003:np). The Sixth Amendment addresses the right to a fair and speedy trial, as well as the right to have the assistance of counsel for the individual's defense. These amendments are stated in full in Chapter 4. There are no more fundamental rights in the United States than those stated in the Bill of Rights. Thus, these are the standards that the Federal government must uphold.

Each of the rights guaranteed by the two amendments considered here is vital. However, it is also recognized that efforts to reduce the threat of terrorism may potentially impact these rights. It is the assumption of this study that the preference is to preserve these rights. The SDVF in Figure E-11 is utilized for both the Fifth Amendment and the Sixth Amendment measures to assess the potential impact of a particular strategy.

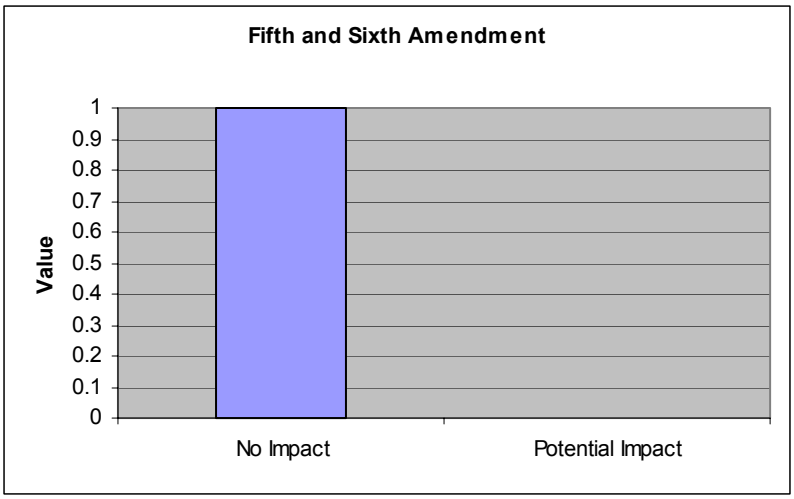

Figure E-11: SDVF for Fifth/Sixth Amendment

The maximum value is provided by a strategy that preserves the rights promised by the amendment in question. When any of the provisions of the Fifth or Sixth Amendment may *potentially* be impacted, the value provided to the decision-maker is zero. Any **definite** reduction of Fifth or Sixth Amendment rights would be a screening attribute. A strategy that does infringe upon the rights granted by the Bill of Rights would automatically be rejected. A strategy that **potentially** could impact these rights would receive no value on these measures, but may still be considered if there were no definite constitutional issues.

Appendix F: Executive Summary

Modeling Homeland Security: A Value Focused Thinking Approach

Lt Kristopher Pruitt, Dr. Richard Deckro, Capt Stephen Chambal, PhD
Air Force Institute of Technology

Problem Statement: The attacks on September 11th, 2001 underscored the rising threat of terrorism within the United States. Since that date, the Federal government has pursued an array of security measures to address the mounting threat. This decision process could benefit from a structured methodology demonstrating how these pursuits are fulfilling the goals of homeland security (HLS). This research provides Federal level HLS decision-makers with a decision support structure, based on Value Focused Thinking (VFT), to leverage in the development and evaluation of alternative strategies.

Research Methodology: The most vital step in any analysis process is problem identification. The main focus of this research is the security of the American homeland. Additionally, the positive consequences of HLS are considered in concert with the potential negative impacts; namely excessive resource costs and infringements on civil liberties. These three concepts, security, resource costs, and civil liberties are balanced against one another.
After problem identification, a value hierarchy is created. This structure specifies lower level objectives that evaluate the fulfillment of upper level objectives. The objectives of HLS are identified through a content analysis of these five documents: The National Strategy for HLS, The Dept of HLS, EO 13228, Securing the Homeland: Strengthening the Nation, and ANSER's Strategic Cycle. This analysis identified 363 HLS objectives that are organized into a hierarchical structure utilizing Affinity Grouping.

Evaluation measures are developed for the lowest tier objectives. The measures provide a quantitative assessment of the qualitative values in the hierarchy. These measures may consist of differing units; therefore, single dimension value functions (SDVFs) convert all measures to a unitless scale, between 0 and 1. In addition, varying measures and objectives may have dissimilar levels of importance. The hierarchy is weighted to reflect the relative importance of each objective and then combined with the resultant 0-1 value score. This provides an overall score for how well a proposed security strategy supports the fundamental objective of HLS.

Model for Homeland Security: Decision-makers must balance securing the United States from terrorism against the required resource costs and the impact on civil liberties. Three distinct value hierarchies model these concepts, starting with security (Fig 1).

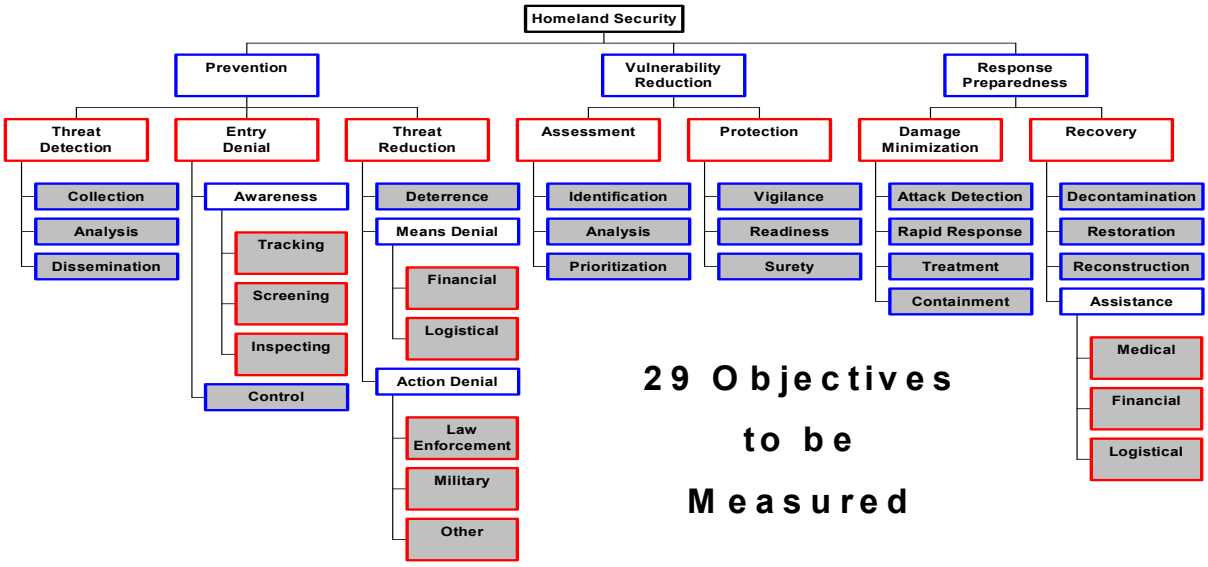

Figure 14: Security Value Hierarchy

The National Strategy for HLS defines homeland security as a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, minimize the damage and recover from attacks that do occur. This definition reflects the overarching objectives of HLS and provides the foundation for the value hierarchy. These values are further specified and result in 29 lowest tier objectives to be measured (shaded blocks in Fig 1).

The 29 objectives define the focus areas that competing strategies are measured against to increase HLS based on improving our current capabilities in these areas. The capability continuum (Fig 2) is defined by the appropriate subject matter experts (SMEs).

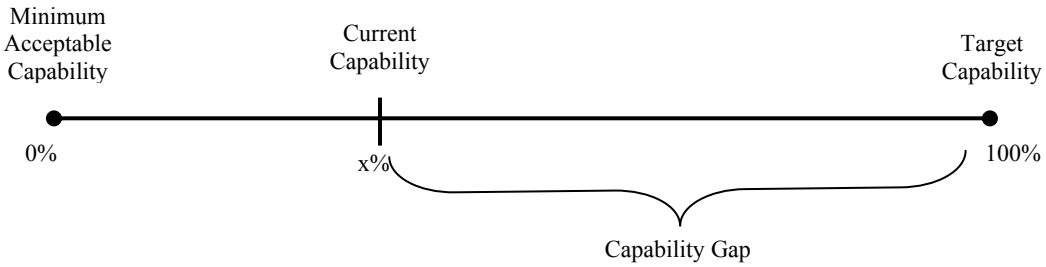

Figure 21: Capability Continuum

The continuum defines targets capabilities and minimum requirements for each measure. The endpoints are specific to each objective and provide a framework for numerically evaluating the current capability. The "capability gap" represents room for improvement; the more a proposed strategy closes this gap, the more valuable it becomes. This capability-based evaluation emphasizes those areas where the Federal government has lower capability. The capability continuum is translated to an exponential SDVF ($V_i(x)$), parameterized by current capability (C_i), measuring the value achieved by a proposed strategy.

$$V_i(x) = \begin{cases} 1, & \text{for } C_i = 100 \\ \dfrac{x}{100}, & \text{for } C_i = 50 \\ \dfrac{1 - e^{-x \cdot R}}{1 - e^{-100 \cdot R}}, & \text{otherwise} \end{cases}$$

where $R = \dfrac{50 - C_i}{\rho}$, for $\rho > 0$.

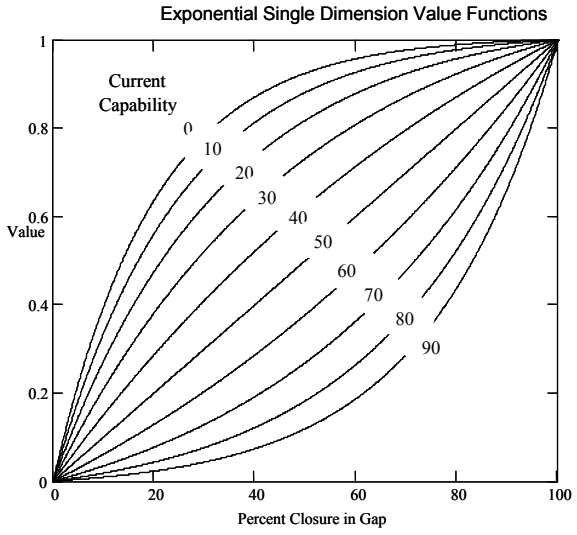

Figure 16: Exponential Single Dimension Value Functions

The value achieved by an x% closure in the capability gap is computed with the appropriate SDVF. If current capability is 100% of the desired target capability, no gap exists and proposed strategies score a 1 in value, assuming no decrease in capability. The parameter rho in the calculation of R determines how drastic the curves become as current capability moves away from 50%. Rho is defined as 1000 to provide a more uniform spread in the current capability curves (Fig 3). If current capability is relatively low (below 50%), small percent closures in capability gap receive a high value. If current capability is high (above 50%) then the gap must be significantly closed to achieve high value. The final step is to weight the hierarchy based on risk, SME, and decision-maker preference. For the notional example, equal weighting is assumed.

The remaining two hierarchies consider resource costs and civil liberties (Fig 4 & 5).

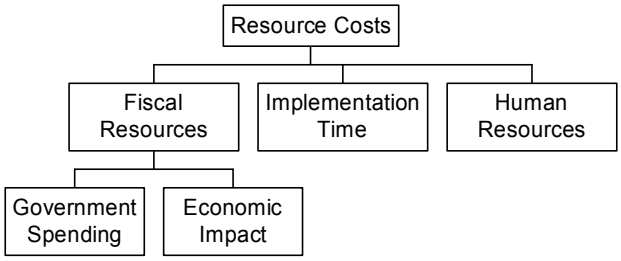

Figure 4: Resource Costs Hierarchy

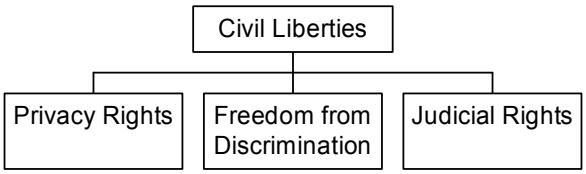

Figure 5: Civil Liberties Hierarchy

Resource costs include monetary aspects, along with the time and personnel required to carry out proposed security strategies. Civil liberties represent the freedoms that define this nation. As with the security hierarchy, evaluation measures determine how well a proposed strategy performs with respect to resource costs and civil liberties. Eight measures are defined for resource costs while five measures are defined for civil liberties. As examples, measures are developed for implementation time under resource costs and privacy rights under civil liberties (Fig 6 & 7).

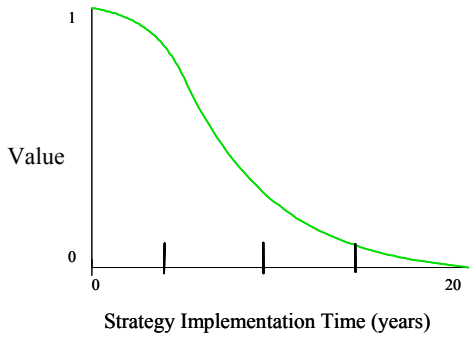

Figure 6: Measure for Implementation Time

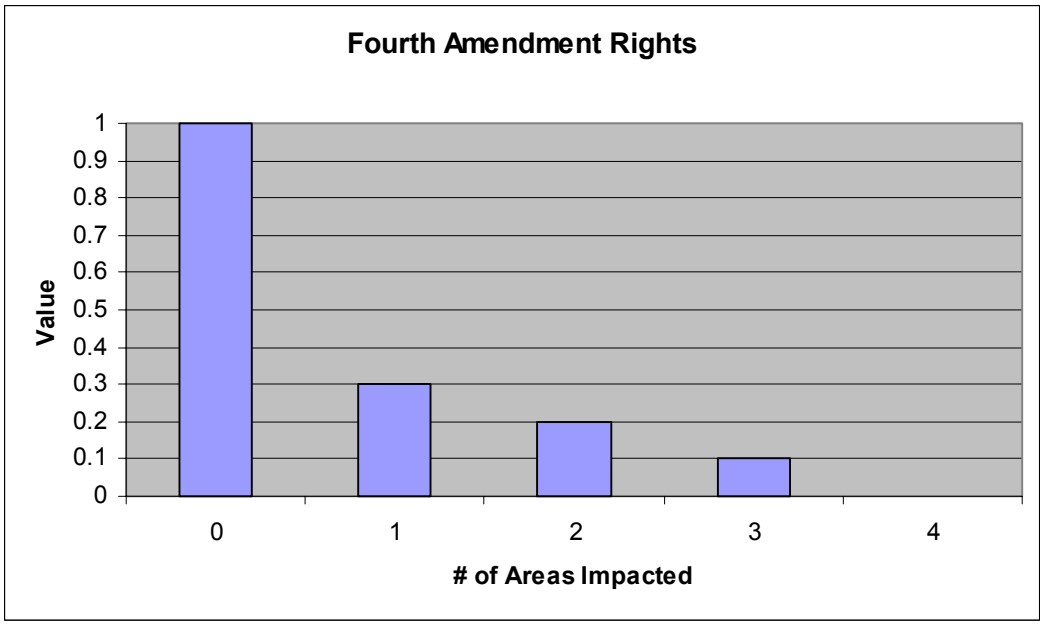

Figure 7: Measure for Privacy Rights

The driving question for implementation time is, "How many years are required to implement all portions of the proposed strategy?" It is assumed that a proposed strategy requiring more than 20 years to implement would be ineffective and receives zero value. In addition, implementation times of five years and less receive high value, while times beyond five years lose value quickly.

The driving question for privacy rights is, "What is the potential impact of the proposed strategy on Fourth Amendment rights?" This amendment protects Americans from illegal searches of their person, their house, their papers, or their effects. The value achieved by a proposed strategy is measured with respect to how many of these four areas it might *potentially* impacts. If a strategy potentially impacts an individual's privacy in any one of these areas it loses value quickly, from 1 to .3. It loses even more value for two areas, three areas, and has no value if it impacts all four.

Example Application: An example illustrates how this research can be applied. Two notional HLS strategies are scored according to their fulfillment of values included in the three hierarchies. The first strategy is the development of a National ID Card. This strategy would require every United States citizen to carry identification at all times which includes their picture, thumbprint, and an array of personal information. The second strategy is the development of detection equipment to inspect shipping containers on aircraft. Such devices would have the capability to detect radiation within a container before it is opened.

Both strategies are scored against all 29 measures in the security hierarchy. Depending on the measure, the strategy may or may not provide an increase in capability. As examples, the National ID Card is scored against screening capability and the detection equipment is scored against inspection capability. Screening involves the capability to observe, identify, and report information pertaining to people and goods. Suppose the current capability to execute this mission is notionally set at 30% on the capability continuum. In addition, suppose the development of the National ID Card increases this capability to 65%. This provides a 50%

closure in the capability gap and achieves a high value of 0.73 (Fig 8). Inspection capability involves the physical verification of the security of people and goods. Suppose current capability is notionally set at 70% and the detection equipment increases capability to 85%. This also equates to a 50% closure in the capability gap. However, unlike the enhancement in screening, it receives a much lower value of .27 (Fig 9).

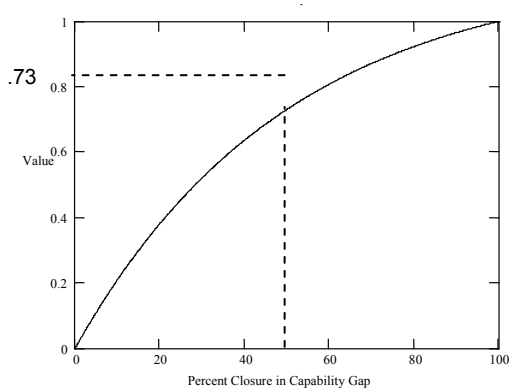

Figure 8: National ID Card - Screening

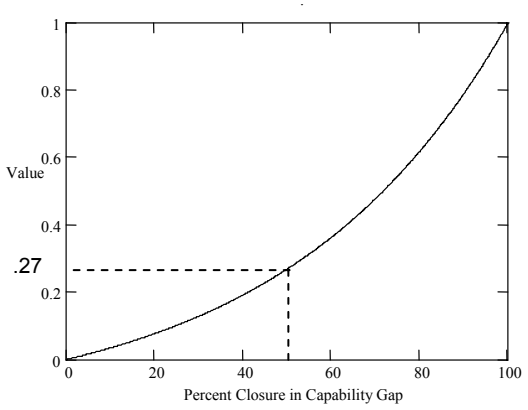

Figure 9: Detection Equipment - Inspecting

Both alternatives are scored for all measures in the resource costs hierarchy. As an example, implementation time is scored. Suppose the National ID requires 10 years to fully implement. Accordingly, the SDVF provides a value of 0.28 (Fig 10). Alternately, suppose the shipping container detection equipment is fully developed and fielded in 3 years. This implementation time achieves a very high value of .91 (Fig 11).

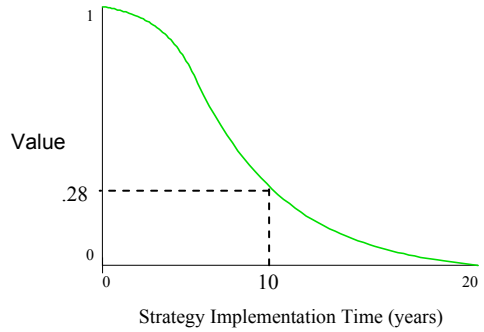

Figure 10: National ID Card - Implementation Time

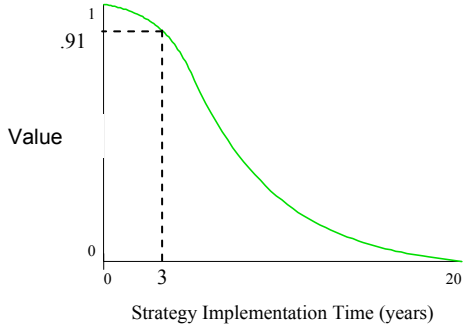

Figure 11: Detection Equipment - Implementation Time

Finally, both alternatives are scored against all measures in the civil liberties hierarchy. As an example, the measure for privacy rights is scored. Suppose the National ID card potentially impacts 3 areas of the Fourth Amendment. Accordingly, it has a very low value of .1 (Fig 12). In contrast, the shipping container detection equipment likely has no impact on privacy rights and achieves the full value of 1 (Fig 13).

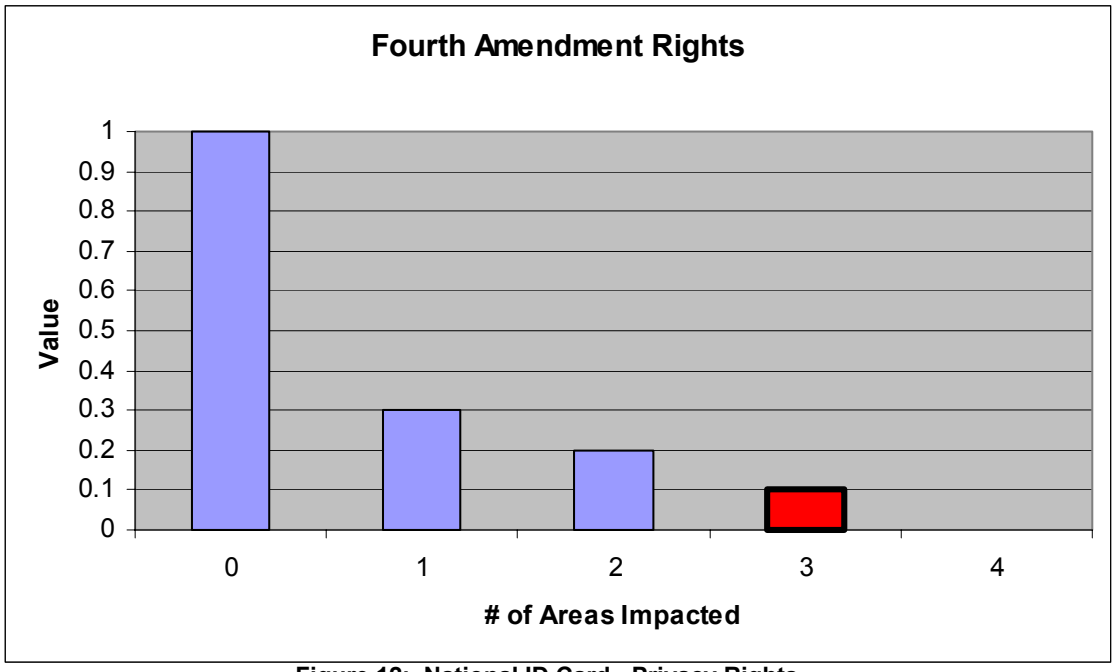

Figure 12: National ID Card - Privacy Rights

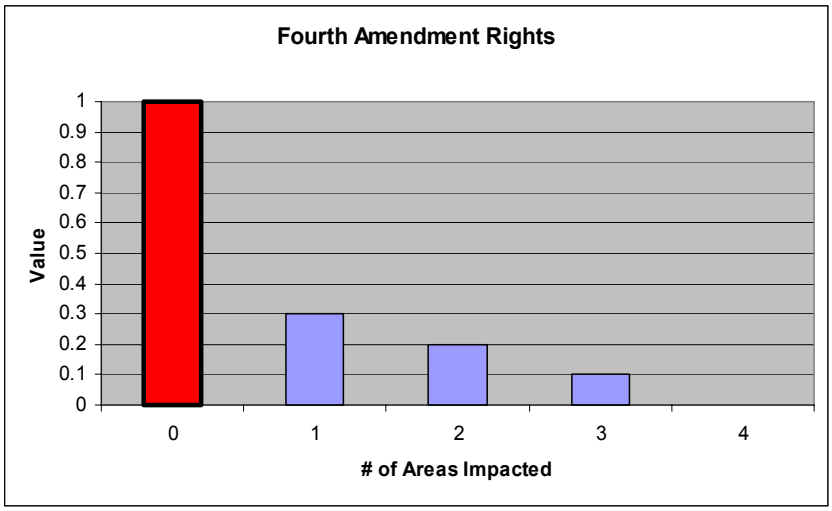

Figure 13: Detection Equipment - Privacy Rights

The proposed strategies (National ID Card and detection equipment) are scored against all the measures in the three hierarchies (security, resource costs, and civil liberties). The values achieved for each measure are combined with the weights to calculate an overall score for each hierarchy. This calculation involves the simple sum-product shown below.

$$\textbf{Overall Value} = \sum_{i=1}^{n} w_i \cdot V_i(x)$$

In other words, the ID card achieves one score, between 0 and 1, for the security hierarchy, one score for the resource costs hierarchy, and one score for the civil liberties hierarchy. The same is true for the detection equipment. This facilitates the trade-offs between security, resource costs, and civil liberties (Fig 14).

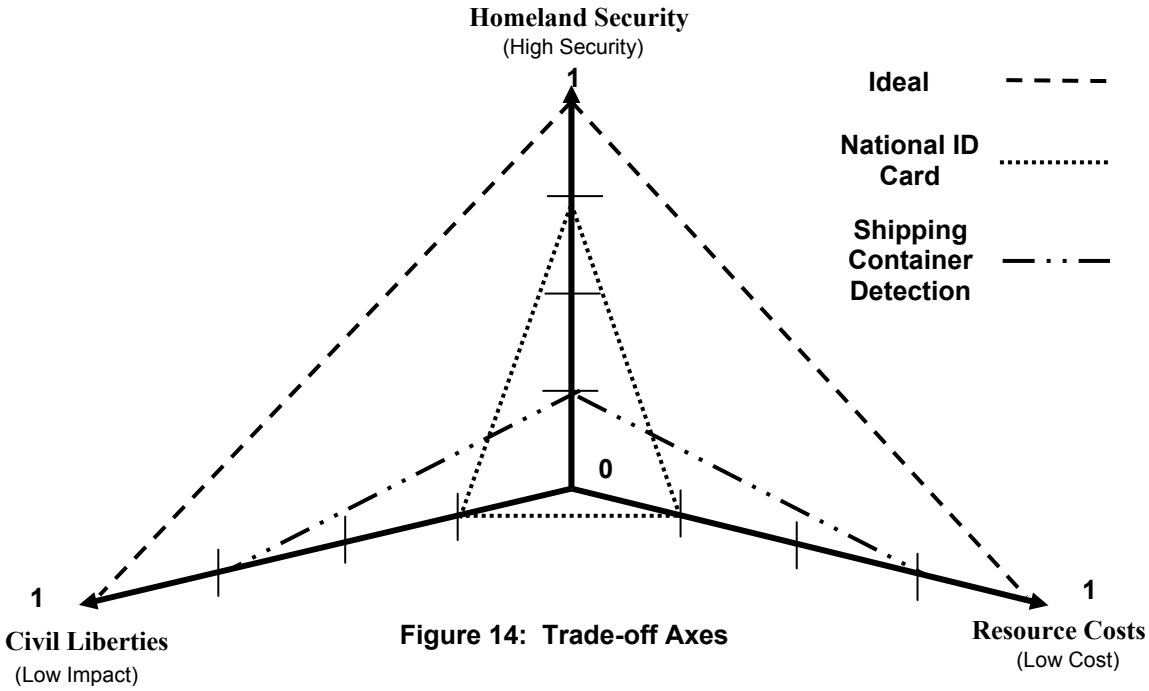

Figure 14: Trade-off Axes

The ideal case is for the strategy to score a 1 for each hierarchy. Such an alternative provides high security at a low cost and a low impact on civil liberties. In this notional example, the National ID Card performs well with respect to security, but is costly and potentially has a high impact on civil liberties. In contrast, the shipping container detection equipment performed very well with respect to cost and civil liberties. Unfortunately, it provides very little increase in the capability to secure the homeland.

Conclusions: As critical infrastructures and key assets remain vulnerable, terrorists' deadly intentions drive HLS to remain of imminent concern. This methodology provides insight into the difficult decision process of allocating scarce resources to the development of effective HLS strategies. While individual strategies were illustrated, combined strategy packages can be evaluated. The hierarchies, particularly the resource costs and civil liberties hierarchies, could certainly benefit from expanded development and added insight of high level experts. However, as is, the Federal government is provided with a significant foundation to leverage in the continuing effort to secure the American homeland from terrorism.

Reference: Pruitt, Kristopher Adam. *Modeling Homeland Security: A Value Focused Thinking Approach*. MS thesis, AFIT/GOR/ENS/03M-19. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2003.

Point of Contact: Capt Stephen Chambal, Phone: (937) 255–6565 x4314, Email: stephen.chambal@afit.edu and Dr. Richard Deckro, Phone: (937) 255-6565 x4325, Email: richard.deckro@afit.edu.

Bibliography

1. Advisory Panel to Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction. *First Annual Report to the President and Congress: Assessing the Threat*. 15 December 1999.

2. Advisory Panel to Assess Domestic Response Capabilities For Terrorism Involving Weapons of Mass Destruction. *Second Annual Report to the President and Congress: Toward a National Strategy for Combating Terrorism*. 15 December 2000.

3. Air University. *SPACECAST 2020: Executive Summary*. Maxwell AFB Alabama: AETC, 22 June 1994.

4. Air University. *SPACECAST 2020: Operational Analysis*. Maxwell AFB Alabama: AETC, 22 June 1994.

5. ANSER Institute for Homeland Security. "Homeland Security: The Strategic Cycle." *Homeland Security 2005: Charting the Path Ahead.* 6-7 May 2002. http://www.homelandsecurity.org/hls/strategycycle.doc

6. Area Education Agency 7. "Affinity Process." School Improvement by Design. November 2002. http://edservices.aea7.k12.ia.us/sibd/community/affinityprocess.html

7. Auster, Bruce. "High Tech Hunting." *ASEE prism*. January 2003. pgs 22-27.

8. Ball, Robert E. "Designed to Survive." *National Aviation News*. November-December 1998. pgs 24-28.

9. Beauregard, Joseph Edward. *Modeling Information Assurance*. MS thesis, AFIT/GOR/ENS/ 01M-03. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2001.

10. Bureau of Reclamation. "Affinity Diagrams." Decision Process Guidebook. November 2002. http://www.usbr.gov/guide/toolbox/affinity.htm

11. Bush, George W. *The Department of Homeland Security*. Washington: The White House, June 2002.

12. Bush, George W. *Securing the Homeland Strengthening the Nation*. Washington: The White House, 2002.

13. CERN: European Organization for Nuclear Resources. "Affinity Diagram." Technical Support Division. November 2002. http://st-div.web.cern.ch/st-div/qa/minutes/QWG-990617/affin.html

14. Chambal, Stephen P. Class notes, OPER 643, Advanced Decision Analysis: Multiple Objective Decision Analysis. School of Engineering and Logistics, Air Force Institute of Technology, Wright-Patterson AFB OH, Summer Quarter 2002.

15. Clemen, Robert T. and Reilly, Terence. *Making Hard Decisions (with DecisionTools®)*. Pacific Grove CA: Duxbury, 2001.

16. Cole, David. "Enemy Aliens and American Freedoms." *Nation*. 23 September 2002. http://www.globalpolicy.org/wtc/liberties/2002/0923nation.htm

17. Cole, David. *Terrorizing the Constitution*. 10 October 2002. http://past.thenation.com/issue/960325/0325cole.htm

18. Constitutional Amendments 1-10: The Bill of Rights. 20 January 2003. http://www.archives.gov/exhibit_hall/charters_of_freedom/bill_of_rights/amendments_1-10.html

19. The Constitution of the United States of America. 11 December 2002. http://www.law.cornell.edu/constitution/constitution.preamble.html

20. Daalder, Ivo H. and others. *Assessing the Department of Homeland Security*. Washington: The Brookings Institution, July 2002.

21. David, Ruth A. *Homeland Insecurity: In Pursuit of the Asymmetric Advantage*. Committee on National Security Systems 2002 Annual Conference. "The CNSS Role in Homeland Security." 9-11 April 2002.

22. Deloitte Consulting. "The Homeland Security Market: The World's Most Challenging Emerging Business Environment." *A Research Report by Deloitte Consulting and Aviation Week*. Report Supplement: Market Size Projections. 5 June 2002.

23. Department of Defense. *Dictionary of Military and Associated Terms*. Joint Publication 1-02. Washington: JCS, 12 April 2001.

24. Department of Defense. *Mandatory Procedures for Major Defense Acquisitions (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs*. DOD 5000.2-R. Washington: OUSD, 10 June 2001.

25. EPIC and Privacy International. *Privacy and Human Rights 2002*. September 2002. http://www.privacyinternational.org/survey/phr2002/

26. Gross, Roberta L. Inspector General Reviews of Presidential Decision Directive 63 Implementation. 12 September 2001.

27. Hamill, Jonathan Todd. *Modeling Information Assurance: A Value Focused Thinking Approach*. MS thesis, AFIT/GOR/ENS/00M-15. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2000.

28. Human Rights and Equal Opportunity Commission (HREOC). Complaint Line: To Complain About Discrimination or Harassment. 10 February 2003. http://www.complaintline.com.au/discrimination.html

29. Jackson, Jack A. Jr., Brian L. Jones, and Lee J. Lehmkuhl. *An Operational Analysis for Air Force 2025: An Application of Value-Focused Thinking to Future Air and Space Capabilities*. Maxwell AFB: Air University Press, May 1996. http://www.au.af.mil/au/2025/volume4/chap03/v4c3-02c.htm

30. Jackson, Jack A. Jr., Brian L. Jones, and Lee J. Lehmkuhl. *An Operational Analysis for 2025*. Maxwell AFB: Air University Press, October 1996.

31. Jordan, Terry L. *The U.S. Constitution and Fascinating Facts About It*. Naperville IL: Oak Hill Publishing, 1999.

32. Kahraman, Yucel R. *Robust Sensitivity Analysis for Multi-Attribute Deterministic Hierarchical Value Models*. MS thesis. AFIT/GOR/ENS/02-10. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2002.

33. Kalyani. "Privacy under Greater Threat after 9/11: Report." *One World South Asia*. 5 December 2002. http://www.globalpolicy.org/wtc/liberties/2002/1205privacy.htm

34. Keefer, Donald L. and others. *Decision Analysis Applications in the Operations Research Literature, 1990-1999*. July 2000. http://www.public.asu.edu/~kirkwood/Papers/DAAppsSummaryTechReport.pdf

35. Keeney, Ralph L. and Raiffa, Howard. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. New York: John Wiley & Sons, 1976.

36. Keeney, Ralph L. *Value-Focused Thinking: A Path to Creative Decisionmaking*. Cambridge MA: Harvard University Press, 1992.

37. Keeney, Ralph L. and McDaniels, Timothy L. "Value-Focused Thinking about Strategic Decisions at BC Hydro." *INTERFACES*. No. 22, 6 Nov-Dec, pp. 94-109, 1992.

38. Keeney, Ralph L. "Countering Terrorism: The Clash of Values." *OR/MS Today*. INFORMS: Volume 28, Number 6, December 2001.

39. Kingsley, Steve. "Homeland Security Act Approved." *Homeland Defense Journal*. Volume 1, Issue 21. 20 November 2002.

40. Kirkwood, Craig W. *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets*. Belmont CA: Wadsworth Publishing, 1997.

41. Lane, Charles. "Has Bush infringed the constitution? The debate heats up." Washington Post. 23 September 2002. http://www.globalpolicy.org/wtc/liberties/2002/0903debate.htm

42. Larsen, Col. Randall J. (Ret.) and David, Ruth A. Homeland Defense: *Assumptions First, Strategy Second*. Journal of Homeland Security. ANSER Institute, October 2000. http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=8#_ednref5

43. Larsen, Randy and Dave McIntyre. *A Primer on Homeland Security: Overview*. ANSER Institute of Homeland Security. November 2002. http://www.homelandsecurity.org/bulletin/overview.htm

44. Larsen, Randy and Dave McIntyre. *A Primer on Homeland Security: Strategic Functions, Threats and Mission Areas*. ANSER Institute of Homeland Security. November 2002. http://www.homelandsecurity.org/bulletin/strategic_functions.htm

45. Lavin, Tim and Sage Stossel. "Security Versus Civil Liberties." *The Atlantic*. 6 February 2002. http://www.globalpolicy.org/wtc/liberties/2002/0206sec.htm

46. Lesser, Ian O. and others. *Countering the New Terrorism*. Santa Monica CA: RAND Project Air Force, 1999.

47. Liptak, Adam, Neil A. Lewis, and Benjamin Weiser. "After Sept. 11, a Legal Battle Over Limits of Civil Liberty." New York Times. 4 August 2002. http://www.globalpolicy.org/wtc/liberties/2002/0804battles.htm

48. Martin, Glen T. "Without Protest, Americans Giving Up Freedom." *Indymedia*. 2 January 2003. http://www.globalpolicy.org/wtc/liberties/2003/0102protest.htm

49. McIntyre, Dave. *Winning this One – The Logic of Homeland Security*. ANSER Institute of Homeland Security. 16 September 2001. http://www.homelandsecurity.org/bulletin/Primer_WinningthisOne.htm

50. McIntyre, Dave. *ANSER Summary and Analysis: A Quick Look at the Proposed Department of Homeland Security*. ANSER Institute for Homeland Security. June 2002. http://www.homelandsecurity.org

51. McIntyre, Dave. *What is to be Done: The Complexity of Homeland Security.* July 2002. http://www.homelandsecurity.org/bulletin/ActionPlan_WhatbeDone.htm

52. McIntyre, Dave. *What is Homeland Security?: A Short History*. ANSER Institute of Homeland Security. November 2002. http://www.homelandsecurity.org/bulletin/ActionPlan_WhatIsHLS.htm

53. Nichols, John. "The Poindextering of Privacy Rights." *Nation*. 21 November 2002. http://www.globalpolicy.org/wtc/liberties/2002/1121poindextering.htm

54. Office of Homeland Security. *National Strategy For Homeland Security*. Washington: The White House, 16 July 2002.

55. Office of the Secretary of Defense. *Proliferation: Threat and Response*. Washington: Department of Defense, January 2001.

56. 107th Congress. First Session. *USA PATRIOT Act*. H.R. 3162. 24 Oct 2001. http://www.epic.org/privacy/terrorism/hr3162.html

57. Orfelio, G. Leon. "Value-Focused Thinking versus Alternative-Focused Thinking: Effects on Generation of Objectives." *Organizational Behavior and Human Decision Processes*. Vol. 80, No. 3, December, pp. 213-227, 1999.

58. Parnell, G., Engelbrecht, J., Szafranski R., & Bennett, E, "Improving Customer Support Resource Allocation", *Interfaces*, Vol 32, No. 3, May-June 2002, pp. 77-90.

59. The President. *Establishing the Office of Homeland Security and the Homeland Security Council*. Executive Order 13228. Washington: Federal Register Vol. 66, No. 196, 8 Oct 2001.

60. The President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Washington: 13 October 1997.

61. The President's Commission on Critical Infrastructure Protection. *Critical Foundations-Thinking Differently*. 1997. http://www.ciao.gov/resource/pccip/summary.pdf

62. Presidential Decision Directive 39. *U.S. Policy on Counter-terrorism*. Washington: The White House, 21 June 1995. http://www.fas.org/irp/offdocs/pdd39.htm

63. Presidential Decision Directive 62. *Combating Terrorism: Fact Sheet*. Washington: The White House, 22 May, 1998. http://www.fas.org/irp/offdocs/pdd-62.htm

64. Reno, Janet. Memorandum on Critical Infrastructure Security. Washington: Office of the Attorney General, 14 March 1996. http://www.fas.org/sgp/othergov/munromem.htm

65. Report of the National Commission on Terrorism. *Countering the Changing Threat of International Terrorism*. 7 June 2000.

66. Report of the National Defense Panel. *Transforming Defense: National Security in the 21st Century*. December 1997.

67. Schorr, Daniel. "Uncivil Liberties." *Christian Science Monitor*. 30 August 2002. http://www.globalpolicy.org/wtc/liberties/2002/0830liberties.htm

68. Stemler, Steve. "An overview of content analysis." *Practical Assessment, Research & Evaluation*, 7(17), 7 June 2001. http://ericae.net/pare/getvn.asp?v=7&n=17

69. Texas Tech University. Affinity Diagramming Slideshow. Department of English. November 2002. http://english.ttu.edu/spinuzzi/5377online/affinity.ppt

70. The United States Commission on National Security/21st Century. *New World Coming: American Security in the 21st Century*. 15 September 1999.

71. The United States Commission on National Security/21st Century. *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom*. 15 April 2000.

72. The United States Commission on National Security/21st Century. *Road Map for National Security: Imperative for Change*. 31 January 2001.

73. U.S. Department of Homeland Security. *DHS Organization*. 3 February 2003. http://www.dhs.gov/dhspublic/display?theme=9

74. University of Massachusetts, Amherst. "Affinity Diagram or the KJ method." Mechanical and Industrial Engineering Department. November 2002. http://mielsvr2.ecs.umass.edu/virtual_econ/module2/affinity_diagram.htm

75. "War on Terror Infringing Human Rights, UNHCR Says." *Reuters*. 17 December 2002. http://www.globalpolicy.org/wtc/liberties/2002/1217unhcr.htm

76. Wolf, Paul. *CIA Powers and 1975 Church Committee*. 22 September 2001. http://www.labournet.net/world/0109/us15.html

Vita

Second Lieutenant Kristopher A. Pruitt graduated from Greencastle High School in Greencastle, Indiana. He entered undergraduate studies at Purdue University in West Lafayette, Indiana where he graduated with a Bachelor of Science degree in Mathematics in May 2001. He was commissioned through the Detachment 220 AFROTC at Purdue University where he held the position of Cadet Wing Commander his final semester.

In August 2001, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology to pursue a Masters of Science in Operations Research. Upon graduation, he will be assigned to the Air Force Logistics Management Agency.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
25-03-2003	**Master's Thesis**	Jun 2002 – Mar 2003

4. TITLE AND SUBTITLE
MODELING HOMELAND SECURITY: A VALUE FOCUSED THINKING APPROACH

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Pruitt, Kristopher A., Second Lieutenant, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GOR/ENS/03-19

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The events of September 11, 2001 have propelled the topic of homeland security to the forefront of national concern. The threat of terrorism within the United States has reached an unprecedented level. The pervasive vulnerabilities of the nation's critical infrastructure coupled with the destructive capabilities and deadly intentions of modern terrorists pose extraordinary risks. The United States must mitigate these risks while at the same time balancing the associated costs and impact on civil liberties.

Currently, the United States lacks effective methods and measures for assessing the security of the homeland from acts of terrorism. This study outlines a first cut decision analysis methodology for identifying and structuring key homeland security objectives and facilitating the measurement of the United States' capability to execute these objectives.

15. SUBJECT TERMS
Homeland Security, Critical Infrastructure Protection, Terrorism, Decision Analysis, Value Focused Thinking, Operations Research

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Stephen P. Chambal, Capt, USAF (ENS)
U	**U**	**U**	**UU**	237	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4314; e-mail: Stephen.Chambal@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18